CYBERNETICA

Avalik

Privaatsuskaitse tehnoloogiate Eestis rakendamise teekaart

Aruanne

Versioon 1.1

31.03.2023

ID D-16-215

Projektijuhid: Liina Kamm (Cybernetica AS)
Nele Nisu (Majandus- ja Kommunikatsiooniministeerium)

Autorid: Dan Bogdanov (Cybernetica AS)
Eduardo Brito (Cybernetica AS)
Paula Etti (Cybernetica AS)
Liina Kamm (Cybernetica AS)
Peeter Laud (Cybernetica AS)
Tanel Mällo (Cybernetica AS)
Andre Ostrak (Cybernetica AS)
Kati Sein (Cybernetica AS)
Riivo Talviste (Cybernetica AS)
Maria Toomsalu (Cybernetica AS)

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Estonia.

E-post: info@cyber.ee, Veebileht: https://www.cyber.ee, Telefon: +372 639 7991.

Sisukord

1 Sissejuhatus

1.1 Motivatsioon

Mis oleks, kui Eesti oskaks ehitada mitmete inimeste või organisatsioonide andmete peal põhinevaid teenuseid sama turvaliselt kui üksikisiku teenuseid üle X-tee? Kui andmete töötlemisel oleks tagatud läbipaistvus ja privaatsus? Kui andmeid oleks võimalik erinevate osapoolte vahel töödelda ilma üksikisikule viitavaid andmeid avaldamata? Millised uued võimalused sellisest võimekusest Eestile avaneda võiksid?

Eesti on tuntud kui riik, kus rakendatakse laialdaselt tehnoloogiat. Andmete kogumise ja töötlemise suurenemisega muutuvad privaatsusküsimused üha olulisemaks.

Turvaline andmekasutus, näiteks privaatsuskaitse tehnoloogiate rakendamine lõimitud andmekaitse osana, võimaldaks arendada uusi kvaliteetseid e-riigi teenuseid ja viiks ühtlasi lähemale inimkesksemale e-valitsemisele. Nii on võimalik muuta protsesse efektiivsemaks ja hoida kokku nii ajalist kui ka rahalist ressurssi. Näiteks oleks võimalik määrata inimestele toetuseid vajaduspõhiselt vastavalt nende tegelikele kuludele, ühendades selleks avaliku ja erasektori andmeid.

Lisaks eelnevale võimaldaks turvaline andmekasutus ja sellel põhinev andmete analüüs tuge riigijuhtidele läbimõeldud otsuste langetamiseks.

Veelgi enam, teaduskoostöö uute tervishoiu-, finants- või muude teenuste loomiseks riigi, teadusasutuste ja ettevõtete vahel edeneks nii Eesti sees, Euroopas kui ka väljaspool. Erasektoris ja teadusasutustes oleks tänasega võrreldes võimalik oluliselt ulatuslikumalt töödelda andmeid, tagades inimeste privaatsuse, uuringuteks, teenuste osutamiseks ja andmepõhiseks otsustamiseks.

See pakuks ainest ka uute äriideede sünniks ja aitaks kaasa uute ettevõtete loomisele, aidates kaasa uute e-residentide ja ettevõtete tekkimisele, tooks riigile maksutulu ja välisinvesteeringuid ning hoiaks Eesti tugevat digiriigi kuvandit.

Lisaks toetaks privaatsusküsimuste lahendamine andmemajanduse kasvu läbi ulatuslikuma andmete kasutuse ja väärindamise. Üldiselt võib privaatsuskaitse tehnoloogiate rakendamine Eestis viia turvalisema ja usaldusväärsema digitaalse keskkonna loomiseni, mis soodustab innovatsiooni, digiriigi arengut ja ettevõtlust, samal ajal kaitstes inimeste õigusi.

Nende unistuste täitmiseks on teadlased ja insenerid aastaid arendanud privaatsuskaitse tehnoloogiaid (ingl k **privacy enhancing technologies**, edaspidi lühendina PET).

1.2 Uuringu lühitutvustus

2022. aastal algatatud Eesti privaatsuskaitse tehnoloogiate uuringul on kaks väljundit.

1. **Privaatsuskaitse tehnoloogiate kontseptsioon** kirjeldab tehnoloogiaid ja pakub üldised mudelid ning kontseptsiooni nende rakendamiseks e-riigis.
2. **Privaatsuskaitse tehnoloogiate Eestis rakendamise teekaart** (see dokument) kirjeldab privaatsuskaitse õigusruumi, intervjuude põhjal Eesti avaliku sektori asutuste kogemust privaatsuskaitse tehnoloogiatega ja vajadusi ning pakub välja poliitikasoovituste ja vastavate arendustegevuste plaani 2023. aasta seisuga.

Uuringu lugeja võib valida, millisest dokumendist ta uuringu tulemitega tutvumist alustab. Tee-

kaardist alustades saab lugeja kõigepealt teada, milliseid privaatsuskaitse tehnoloogiaid Eestis kasutatud on ja millised on siinse avaliku sektori organisatsioonide vajadused. Dokumendi lõpus olev arendusplaan aitab koostada tööplaane ning teha otsuseid investeeringute vajaduse kohta.

Rakendamise kontseptsioonist alustaja saab teada, kuidas privaatsuskaitse tehnoloogiad töötavad, kuidas neid teistes riikides kasutatud on ning milliseid e-riigi probleeme need lahendavad. Mis veelgi tähtsam – rakendamise kontseptsioon kirjeldab, kuidas organisatsioon saab oma arendustsüklis privaatsuskaitse tehnoloogiaid kasutusele võtta.

1.3 Dokumendi käsitlusala

Eesti e-riigi infosüsteemide väärtus luuakse selles liikuvate andmete kaudu. Need andmed on seotud isikute ja organisatsioonidega ning neid töötlevad mitmed asutused. Eesti on olnud pioneer hajutatud teenuste ja andmemudeli juurutamises ning turvatehnoloogiate kasutamises.

Andmete taaskasutus ja uued analüütikarakendused (kratid, sündmusteenused) on Eesti e-riigi arhitektuurile esitanud uusi ülesandeid, mida X-tee loomise ajal veel sellisel kujul ette ei nähtud. Paljude isikute andmete koondamine mitmest allikast, uued andmekaitse ja turvanõuded ning vajadus tagada üha keerukamate süsteemide kvaliteet ja töökindlus nõuavad uute tehnoloogiate kasutuselevõtmist.

Eesti asutused on privaatsuskaitse tehnoloogiaid juba uurinud ja rakendanud. Üheks pikaajaliseks näiteks on Tartu Ülikooli Eesti Geenivaramu, mille tööd määravasse Inimgeeniuuringute seadusesse kirjutati pseudonüümimise nõue sisse juba rohkem kui kakskümmend aastat tagasi.[1] Lihtsamaid tehnoloogiaid on rakendatud juba üle aastate ja saavutatud küpsus, keerukamaid tehnoloogiaid on piloteeritud või arendatud teadusprojektides.

Uuringu käigus intervjueerisid autorid 18 Eesti avaliku sektori asutuse esindajaid ning uurisid privaatsuskaitse tehnoloogiate kasutamise kogemusi, pooleliolevaid projekte ja vajadusi. Selle põhjal on koostatud ka käesoleva dokumendi peatükid 5 (Poliitikasoovitused) ja 6 (Privaatsuskaitse tehnoloogiate rakendamise arendusplaan).

1.4 Mõisted

konfidentsiaalsus (ingl k *confidentiality*)
: üks teabe turvalisuse kolmest põhikomponendist; andmete omadus, mis näitab, mil määral need andmed ei ole volitamata isikutele, protsessidele või muudele olemitele kättesaadavad ega avalikustatud;

käideldavus (ingl k *availability*)
: üks teabe turvalisuse kolmest põhikomponendist; omadus olla volitatud olemi nõudel õigel ajal kättesaadav ja kasutuskõlblik;

lõimitud andmekaitse (ingl k *data protection by design*)
: asjakohaste tehniliste ja korralduslike meetmete rakendamine nii, et saab tõhusalt rakendada andmekaitsepõhimõtteid; vajalike kaitsemeetmete lõimimine isikuandmete töötlemisse, et täita Euroopa Liidu isikuandmete kaitse üldmääruse (edaspidi IKÜM)[2] nõudeid ja kaitsta andmesubjektide õiguseid;

[1] Inimgeeniuuringute seadus, RT I, 13.03.2019, 64, https://www.riigiteataja.ee/akt/113032019064 (viimati külastatud 03.03.2023).

[2] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) [1].

läbipaistvus (ingl k *transparency*)
: süsteemi või protsessi avatus ja jälitatavus; omadus, mis tagab, et kogu privaatsust puudutav andmetöötlus, sealhulgas õiguslik, tehniline ja korralduslik külg oleks arusaadav ja ennistatav;

privaatsuskaitse tehnoloogia(d) (ingl k *privacy enhancing technologies*)
: info- ja sidetehnoloogilised meetmed, tooted või teenused, mis kaitsevad privaatsust isikustatavate andmete välistuse või vähendamisega või isikustatavate andmete tarbetu ja/või soovimatu töötluse vältimisega, samas säilitades süsteemi võimed;

privaatsuslõime (ingl k *privacy by design*)
: süsteemitehniline käsitlusviis, mis arvestab privaatsust kogu süsteemi elutsüklis ning näeb ette privaatsusnõuete esitamist süsteemide, tehnoloogiate, äritavade jms spetsifikatsioonides, võrdle ka mõistega ”lõimitud andmekaitse”;

privaatsustehnika (ingl k *privacy engineering*)
: distsipliin, mis keskendub juhistele, kuidas vähendada privaatsusriske ning põhjendada otsuseid ressursside paigutamiseks ja meetmete toimivaks teostuseks infosüsteemides;

sekkutavus (ingl k *intervenability*)
: omadus, mis tagab, et privaatsust puudutavasse kogu andmetöötlusse saavad sekkuda kohaldatavate õigusaktide tingimustel andmesubjektid, isikutuvastusteabe korraldajad, isikutuvastusteabe töötlejad, järelevalveorganid;

seostamatus (ingl k *unlinkability*)
: ründe või privaatsuse kontekstis on huviobjektid süsteemis seostamatud, kui nende uurimine väljastpoolt ei anna lisateavet nende võimaliku seotuse kohta;

terviklus (ingl k *integrity*)
: üks teabe turvalisuse kolmest põhikomponendist; varade õigsuse ja täielikkuse kaitstus;

vaikimisi andmekaitse (ingl k *data protection by default*)
: tehnilised ja korralduslikud meetmed tagamaks, et töödeldaks üksnes iga konkreetse töötlusotstarbe jaoks vajalikke isikuandmeid.

1.5 Alusmaterjalid

Aruande koostamisel lähtuti järgmistest materjalidest:

1. Arenguseire Keskus, *Andmeühiskonna tulevik. Stsenaariumid aastani 2035* [2];
2. Majandus- ja Kommunikatsiooniministeerium, *Eesti digiühiskond 2030* [3];
3. Ühendkuningriigi akadeemia *The Royal Society* aruanne *From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis* [4];
4. Ühendkuningriigi andme-eetika ja -innovatsioonikeskuse CDEI aruanne *Privacy Enhanching Technologies Adoption Guide* [5];
5. ÜRO komitee *United Nations Committee of Experts on Big Data and Data Science for Official Statistics* aruanne *United Nations Guide on Privacy-Enhancing Technologies for Official Statistics* [6];
6. Cybernetica AS, Privaatsuskaitse tehnoloogiate kontseptsioon, 2023 [7];
7. Erinevate valdkondade teaduskirjandus (täielik ülevaade dokumendi lõpus bibliograafias).
8. Õigusmaastiku analüüs: EL ja Eesti asjakohased õigusaktid, erinevad riigi analüüsidokumendid, Andmekaitse Inspektsiooni ja Euroopa Andmekaitsenõukogu asjaomased suunised.

Teekaardi oluliseks alusmaterjaliks on uuringu käigus teostatud 11 intervjuud 18 asutusega.

1. Intervjuu Andmekaitse Inspektsiooniga. (30.01.2023)
2. Intervjuu Justiitsministeeriumiga. (09.02.2023)
3. Intervjuu Majandus- ja kommunikatsiooniministeeriumi ning Transpordiametiga. (22.02.2023)
4. Intervjuu Maksu- ja tolliameti ning Rahandusministeeriumi Infotehnoloogiakeskusega (RMIT). (14.02.2023)
5. Intervjuu Rahandusministeeriumi ja Finantsinspektsiooniga. (03.02.2023)
6. Intervjuu Riigi Infosüsteemi Ametiga. (31.01.2023)
7. Intervjuu Siseministeeriumi, Politsei- ja Piirivalveameti, Päästeameti ja Siseministeeriumi Infotehnoloogia- ja Arenduskeskusega (SMIT). (08.02.2023)
8. Intervjuu Sotsiaalministeeriumi ja Tervise ja Heaolu Infosüsteemide Keskusega (TEHIK). (09.02.2023)
9. Intervjuu Statistikaametiga. (21.02.2023)
10. Intervjuu Tartu Ülikooli genoomika instituudi Eesti geenivaramuga. (20.02.2023)
11. Intervjuu Tervisekassaga. (06.02.2023)

1.6 Intervjuude metoodika

Et koostatav teekaart (ennekõike selle poliitikasoovitused ja arendusplaan) saaks lähtuda Eesti organisatsioonide reaalsetest vajadustest privaatsust, andmeid või sidet kaitsta, viisime Majandus- ja Kommunikatsiooniministeeriumi tellimusel läbi viia kümme intervjuud Eesti asutustega. Uuringu autorid panid koostöös tellijaga kokku nimekirja organisatsioonidest, kelle töötajatega võiks vahetult vestelda. Selliseid asutusi sai 18. Ühelt poolt arvestades tellija ettepanekut piirduda kümne intervjuuga, teisalt sooviga hinnata asutustevahelist sünergiat, kavandati mitu sama valdkonna asutust ühele intervjuule (vt peatükk 1.5). Intervjuude kutsed saadeti asutustele välja jaanuaris 2023 palvega edastada see kolleegidele, keda teema kõnetab. Kutsele vastasid konstruktiivselt kõik organisatsioonid ja kõik intervjuud said lähema kuu aja jooksul ka teoks (küll selle erinevusega, et üks intervjuu teostus kahes jaos, seega kokku 11 intervjuud).

Kohtumisele eelneval nädalal saadeti intervjueeritavatele tutvumiseks uuringusse kaasatud privaatsuskaitse tehnoloogiate üheleheküljelised kokkuvõtted, mille lõppkujud on leitavad kontseptsiooni dokumendi lõppversioonist [7]. Lisaks palusime intervjueeritavatel mõelda kolmele raamküsimusele.

1. Kuidas teie organisatsiooni/valdkonna igapäevategevusse puutub privaatsuskaitse (või ka andmekaitse)?
2. Missuguseid privaatsuskaitse lahendusi täna rakendate ja miks?
3. Missuguseid teie asutuse/valdkonna (ka piiriülese koostöö) tänaseid väljakutseid võiks lahendada privaatsuskaitse tehnoloogiate abil ja mida positiivset see Eesti ühiskonnale kaasa tooks?

Uuringurühma poolt osales kõigil intervjuudel vähemalt kaks inimest: intervjuu läbiviija vestluse suunaja rollis ja tehniline ekspert, et vajaduse korral tutvustada mõnd tehnoloogiat lähemalt. Asutustest oli vastamas inimesi nii tehnilise ja juriidika poolelt kui äri- ja organisatsioonijuhtimise tasandilt; osalejate ametinimetused: andmekaitsespetsialist, õigusnõunik, andmeteadlane, infoturbe- ja strateegiajuht, arhitekt, tootejuht, ärianalüütik, osakonnajuhataja jne.

Igaks intervjuuks planeeriti 1,5 tundi. Mõni intervjuu kestis veidi kauem, mõni vähem aega. Intervjuud toimusid osaliselt vaid füüsiliste kohtumistena, ent enamasti hübriidkujul: kohtuti kas uuringu korraldaja või intervjueeritava kontoris, kuhu virtuaalsilla vahendusel liitusid need osalejad, kes kohale ei saanud tulla.

Kõik intervjuud protokolliti ning nende põhjal kirjutatud kokkuvõtted saadeti osalejatele järgneva nädala jooksul üle vaatamiseks ja täiendamiseks, mida mitu asutust ka kasutasid. Intervjuude kokkuvõtteid kasutati vajaduspõhiselt raporti erinevate osade informeerimiseks ja sisustamiseks: peamiselt peatükid 3 (Eesti kogemused privaatsuskaitse tehnoloogiatega), 4 (Eesti riigiasutuste privaatsuskaitse-alased vajadused), mis omakorda olid sisendiks peatükkidele 5 (Poliitikasoovitused) ja 6 (Privaatsuskaitse tehnoloogiate rakendamise arendusplaan).

1.7 Aruande struktuur

Peatükis 2 anname ülevaate privaatsuskaitse tehnoloogiate rakendamisega seotud õiguslikest aspektidest, lähtudes eelkõige Euroopa Liidus kehtivatest privaatsuse- ja andmekaitse nõuetest nagu IKÜM. Peatükis kirjeldame, mida peaks jälgima ja arvesse võtma privaatsuskaitse tehnoloogiate rakendamisel.

Peatükis 3 esitame Eesti teenuste ja infosüsteemide ja ehitajate kogemused privaatsuskaitse tehnoloogiatega. Peatükk annab aimu, millised tehnoloogiad on Eestis rohkem ja millised vähem kasutust või tähelepanu leidnud.

Peatükk 4 kirjeldab intervjuude alusel Eesti riigiasutuste esindajate poolt esile toodud vajadusi, mille lahendamisel võiks privaatsuskaitse tehnoloogiatest abi olla. Sealhulgas tuuakse esile võimalusi privaatsuskaitse tehnoloogiate rakendamiseks olemasolevate lahenduste parendamisel ja uute süsteemide juurutamisel.

Peatükk 5 annab poliitikasoovitusi privaatsuskaitse tehnoloogiate kasutuselevõtu otseseks ja kaudseks toetamiseks. Soovitused on ka teiste teemade kohta, mille edukas lahendamine on eelduseks andmemajanduse edendamiseks.

Peatükis 6 kirjeldame, millised võiksid olla järgmised sammud privaatsuskaitse tehnoloogiate arendamisel, juurutamisel ja populariseerisel Eestis ning millist mõju need sammud avaldaksid. Peatükk esitab privaatsuskaitse tehnoloogiate rakendamise arendusplaani, mille loomisel lähtusime intervjuude käigus esile tulnud vajadustest ning lahendustega loodavast lisaväärtusest.

2 Privaatsuskaitse tehnoloogiate rakendamist mõjutav õigusmaastik

2.1 Sissejuhatus

Organisatsioonid ja ettevõtted püüavad oma tööprotsesse muuta efektiivsemaks, kasutades erinevad automatiseerimise ja digitaliseerimise lahendusi, mis omakorda panustavad andmete mahtude suurenemisesse. Andmed on tänapäeval tähtis vara, mille kaitsmine muutub nende koguse kasvuga keerukamaks ja olulisemaks. Kaitset vajavad andmed jaotuvad erinevatesse kategooriatesse lähtuvalt sellest, milliste isikutega neid seostada saab ja milline on nende tundlikkuse aste.

Organisatsioonid ja ettevõtted peavad olema teadlikud tegutsemispiirkonnas kehtivatest privaatsuse ja andmekaitse alastest õigusaktidest. Teadaolevalt on juba 137 riiki kehtestatud asjaomased õigusaktid, et tagada isikute privaatsuse ja andmete kaitse.[3] Isikuandmete töötlemisel tuleb lähtuda privaatsuse ja andmekaitse nõuetest, mis võivad olla jurisdiktsiooniti erinevad. Oluline on tähelepanu pöörata ka eetika ja isiku autonoomia aspektidele. Arvesse tuleb võtta ka isiku põhiõiguseid.

Ettevõtete valduses on palju ka selliseid andmeid, mis ei ole isikuandmed, aga vajavad samuti tõhusat kaitset, näiteks riigisaladus, ärisaladus, intellektuaalomand ja palju muud. Privaatsuskaitse tehnoloogiad (PET), aga ka läbipaistvuse ja sekkutavuse tehnoloogiaid pakuvad nii isikuandmete kui muude andmete kaitsmiseks erinevaid võimalusi. Need on välja töötatud selleks, et vähendada vajadust töödelda süsteemides tuvastatavaid andmeid. PETe on võimalik käsitleda kui õiguslikus mõistes täiendavaid kaitsemeetmed, pakkudes andmetele vajalikul määral kaitset.

Globaliseeruvas andmetöötluses muutub privaatsuskaitse tehnoloogiate kasutamine iga hetkega üha aktuaalsemaks, et kaitsta andmeid ka lubamatu taaskasutuse või väärkasutamise eest. Tehnoloogiliste lisameetmetena aitavad need tehnoloogiad vastata regulatsioonides kehtestatud nõuetele. Andmete kaitsmisel on oluline ka asjakohase kaitsetarbe määramine, et teada, milliseid kaitsemeetmeid oleks otstarbekas kasutada. See omakorda eeldab ka tehniliste kaitsemeetmete hindamist, et oleks võimalik analüüsida, millised on parimad kaitselahendused lähtuvalt konkreetsetest andmetest ja nende kaitsetarbest.

Selleks, et oleks võimalik valida sobivaid ja tõhusaimat kaitset pakkuvaid privaatsuskaitse, läbipaistvuse ja sekkutavuse tehnoloogiaid, on vaja asjakohaseid riskianalüüsi metoodikaid, mis aitaksid mõista erinevate tehnoloogiate kasutamise riske, nõrkuseid ja eeliseid. Kui privaatsuskaitse tehnoloogiaid oleks võimalik kategoriseerida näiteks isiku korduva tuvastamise vältimise taseme järgi, oleks võimalik anda hinnang selle kohta, milline on praegune tehnoloogiate tase ja milliseid neist võiks pidada piisavalt tugevateks, et kaitsta tundlikke ja eriliiki isikuandmeid.

2.2 Andmepõhine Euroopa

Euroopa Liidu (EL) jaoks on privaatsus ja andmekaitse küsimused väga olulised, mistõttu on kehtestatud mitmeid õigusakte vastavate õiguste kaitseks. EL põhiõiguste hartaga (edaspidi harta) reguleeritakse õigusi, mis tulenevad eelkõige liikmesriikide ühistest põhiseaduslikest tavadest ja

[3] UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (viimati külastatud 15.01.2023).

rahvusvahelistest kohustustest, Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist, liidu ja Euroopa Nõukogu poolt vastuvõetud sotsiaalhartadest ning EL Kohtu ja Euroopa Inimõiguste Kohtu praktikast. Harta sisaldab põhiõigustest ka õigust isikuandmete kaitsele (vt harta art 8). Õigust isikuandmete kaitsele sätestab ka EL toimimise lepingu (ELTL) artikli 16 lõige 1.

Euroopa Liit soovitakse muuta andmepõhise ühiskonna liidriks, mis võimaldaks ühtsel andmeturul ELi piires ja valdkondade vahel informatsioonil vabalt liikuda, et luua täiendavat väärtust kogu ühiskonnale. Eesmärgi saavutamiseks on vastu võetud Euroopa Andmestrateegia, kuivõrd andmepõhisel innovatsioonil nähakse suurt potentsiaali[4].

Euroopa Andmestrateegia osana on esitatud mitmeid õiguslikke algatusi. Euroopa andmehalduse määruse[5] eesmärgina on nimetatud vajadust arendada edasi piirideta digitaalset siseturgu ning inimkeskset, usaldusväärset ja turvalist andmeühiskonda ja -majandust (määruse põhjenduspunkt (pp) 3). Lisaks on esitatud seadusandlik ettepanek andmemääruse kehtestamiseks, mis ühtlustab õigusnorme, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist.[6] Andmehalduse määruse pp 3 kohaselt on vaja „parandada andmete jagamise tingimusi siseturul, luues andmevahetuse ühtlustatud raamistiku ja kehtestades teatavad andmehalduse põhinõuded, pöörates seejuures erilist tähelepanu liikmesriikidevahelise koostöö hõlbustamisele. Määruse eesmärk peaks olema arendada edasi piirideta digitaalset siseturgu ning inimkeskset, usaldusväärset ja turvalist andmeühiskonda ja -majandust.“. Avaliku sektori poolt loodud või kogutud andmete üks eesmärk võiks olla väärtuse loomine kogu ühiskonnale (andmehalduse määrus, pp 6).

Tehnoloogia arenguga, eriti digitaalsete andmetöötluse võimalustega seoses omandab avaliku sektori käes olev informatsioon üha rohkem väärtust. Direktiiv (EL) 2019/1024 (avaandmete direktiiv) kehtestati avaandmete kasutamise edendamiseks ning toodete ja teenuste innovatsiooni stimuleerimiseks, mis reguleerivad teatud dokumentide ja andmete taaskasutamist ja nende taaskasutamist soodustavate praktiliste vahendite kasutuselevõttu (artikkel 1 lõige 1). Avaandmete direktiiviga soovitakse tagada, et avaliku sektori asutused teeksid rohkem avaliku sektori teavet kasutamise ja taaskasutamise eesmärgil kergesti kättesaadavaks. Viidatud direktiivi normid on Eesti õigusesse üle võetud avaliku teabe seadusega (AvTS), mille eesmärgiks on tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest, ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle (§ 1).

AvTS § 3^1 reguleerib avaliku teabe taaskasutamist. Selle lõike 1 kohaselt on teabe taaskasutamine füüsilise või juriidilise isiku poolt sellise avaliku teabe kasutamine, mille üldist kasutamist ei ole seadusega või seadusega kehtestatud korras piiratud (edaspidi avaandmed), ärilisel või mitteärilisel eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi. Avaandmetega seondub kindlasti mitmeid küsimusi. Näiteks, kuidas oleks võimalik andmeid efektiivselt süsteemidest kätte saada; kuidas korraldada andmete puhastamine või anonüümimine enne nende avaldamist; kas andmetele on vaja rakendada ka teatud juurdepääsupiiranguid.[7] Mitmeid küsimusi on võimalik lahendada ka privaatsuskaitse

[4] Euroopa Komisjon, Euroopa andmestrateegia, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_et (Viimati külastatud 13.02.2023).

[5] Euroopa Parlamendi ja nõukogu määrus (EL) 2022/868, 30. mai 2022, Euroopa andmehalduse kohta ning millega muudetakse määrust (EL) 2018/1724 (andmehalduse määrus), https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R0868&from=EN

[6] Ettepanek: Euroopa Parlamendi ja nõukogu määrus ühtlustatud õigusnormide kohta, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist (Andmemäärus), https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52022PC0068&from=EN.

[7] Eesti avaandmed, Juhendid, https://avaandmed.eesti.ee/instructions (Viimati külastatud 02.03.2023).

tehnoloogiate abil.

Majandus- ja Kommunikatsiooniministeerium viis 2022. a detsembris läbi avaandmete mõjuhinnangu mitmete avaliku sektori asutuste seas. Mõjuhinnangus on sedastatud, et avaandmete valdkonna edendamine nõuab terviklikku lähenemist, sh tihedat koostööd, olulised on ka tegevuste läbipaistvus, kaasamine ja avatud arutelud. Selles leiti, et enamus organisatsioone ei ole suutnud oma andmeid täies mahus kaardistada. Probleeme on ka andmekvaliteediga. Organisatsioonid püüavad tagada enam kasutatud andmete kvaliteeti, kuid süsteemse mõõtmise asemel tegeletakse pisteliste kontrollidega. Samuti leiti, et andmestike avaldamine toimub juhtumipõhiselt, vahel ei avalikustata isegi avaliku juurdepääsuga masinmõistetavad andmed. Avaandmetega seonduva arengu peamise takistusena nähti inimressursi ning kompetentside ja teadmiste puudumist [8].

Teadmiste rikastamiseks ja andmehalduse paremaks toimimiseks on Eestis välja antud andmehalduse juhised, mis koosneb kolmest peamisest dokumendist – andmehalduse raamistikust, andmekirjelduse juhisest ja andmekvaliteedi juhisest. Andmehalduse raamistik on abiks organisatsiooni andmehalduse protsesside korraldamisel. Andmekirjelduse juhis on abiks erinevate andmekirjeldusega seotud tegevuste puhul, kusjuures juhise lisaks on andmekirjelduse standard, mille järgimine on andmekirjelduste RIHAsse edastamise eelduseks. Andmekvaliteedi juhis on abiks andmekvaliteedi haldamise põhimõtete rakendamisel[9].

Avaandmetega seoses on Euroopa Andmekaitsenõukogu tundnud muret, et ilma tugevate andmekaitsemeetmeteta võib tekkida risk, et digimajandus ei ole kestlik. Kuigi kahtlemata on andmete taaskasutamine, jagamine ja kättesaadavus kasulik, võib see põhjustada ka mitmesugust kahju puudutatud isikutele ja ühiskonnale tervikuna, mõjutades andmesubjekte mitmest vaatenurgast, sh majanduslikust, poliitilisest ja sotsiaalsest[10]. Seetõttu on hästi oluline tegeleda privaatsuskaitse tehnoloogiatega, neid arendada, analüüsida, hinnata, katsetada ja rakendada, et isikud julgeksid oma andmed usaldada turvaliselt riigi kätte.

20. jaanuaril 2023 esitas Euroopa Komisjon seadusandliku ettepaneku Euroopa rahvastiku- ja eluasemestatistika määruse kehtestamiseks[11]. Ettepaneku seletuskirjas on täpsustatud, et kõnealuse algatuse kontekstis tähendab Euroopa rahvastikustatistika ELi tasandi ametlikku statistikat rahvastiku, rahvastikusündmuste ja rände kohta ning sellel statistikal põhinevaid erinevaid näitajaid.

Viidatud ettepanek on privaatsuskaitse tehnoloogiate kontekstis oluline seetõttu, et selles nimetatakse konkreetselt privaatsuskaitse tehnoloogiate katsetamist ja kasutamist[12]. Näiteks on et-

Avaandmed antakse taaskasutamisse üldjuhul tingimusteta, kuid kui tingimused siiski avalikes huvides seatakse, peavad need olema objektiivsed, proportsionaalsed ja mittediskrimineerivad ning kättesaadavad masinloetaval kujul ja avatud vormingus Eesti teabeväravas (AvTS § 3^1 lõige 9).

[8] Eesti avaandmed, Avaandmete mõjuhinnang avalikus sektoris 2022. (02.01.2023) - Internetis kättesaadav: https://avaandmed.eesti.ee/instructions/avaandmete-mojuhinnang-avalikus-sektoris-2022 (Viimati külastatud 02.03.2023).

[9] Kratid.ee, Andmehalduse juhised. - Internetis kättesaadav: https://www.kratid.ee/andmehalduse-juhised (Viimati külastatud 28.02.2023)

[10] Euroopa Andmekaitsenõukogu, Avaldus 05/2021 andmehaldust käsitleva õigusakti kohta seoses õigusloome suundumustega Vastu võetud 19. mail 2021. - Internetis kättesaadav: https://edpb.europa.eu/system/files/2021-08/edpb_statementondga_19052021_et.pdf (Viimati külastatud 02.03.2023).

[11] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb Euroopa rahvastiku- ja eluasemestatistikat ning millega muudetakse määrust (EÜ) nr 862/2007 ja tunnistatakse kehtetuks määrused (EÜ) nr 763/2008 ja (EL) nr 1260/2013, Brüssel, 20.1.2023, COM(2023) 31 final, 2023/0008 (COD), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12958-Data-collection-European-statistics-on-population-ESOP-_en.

[12] Õigusaktide tasandil on soovitatud kasutada ka erinevaid krüpteerimistehnoloogiaid ja vaiketurvet turvalisuse

tepaneku seletuskirja punktis 5 selgitatud, et tõhusa andmete jagamise kvaliteedi võimaldamise huvides kooskõlas isikuandmete kaitse üldmäärusega (edaspidi IKÜM või üldmäärus)[13] nõutakse selliste eraelu puutumatust soodustavate tehnoloogiate katsetamist ja kasutamist, mis on välja töötatud andmekogumise vähendamiseks. Sellest ideest on kantud ka ettepaneku mitmed artiklid[14] ja pp 30:

> *"Kui andmete jagamine eeldab isikuandmete töötlemist vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679 või määrusele (EL) 2018/1725, tuleks täielikult kohaldada eesmärgikohasuse, võimalikult väheste andmete kogumise, säilitusaja piiramise ning tervikluse ja konfidentsiaalsuse põhimõtteid. Otsesele andmeedastusele tuleks eelkõige eelistada eraelu puutumatust soodustaval tehnoloogial põhinevaid andmejagamismehhanisme, mis on nende põhimõtete rakendamiseks välja töötatud."*

Peamine õigusakt, mis reguleerib PET-ide kasutamist EL-is, kui nende kasutamine on seotud isikuandmete töötlemisega, on IKÜM. See kehtestati peamiselt kahe eesmärgi täitmiseks – esiteks, et hõlbustada isikuandmete vaba liikumist ELis, ja teiseks, et säilitada samal ajal füüsiliste isikute põhiõigused ja -vabadused, eelkõige nende õigus isikuandmete kaitsele.[15] See kohaldub mistahes isikuandmete töötlemisele. IKÜMi üheks eesmärgiks, mida kannab selle artikkel 3, on tagada andmesubjektide õiguste tõhus kaitse ELis ja luua ülemaailmsete andmevoogude seisukohast võrdsed tingimused ELis tegutsevatele äriühingutele[16]. Arusaamade ühtlustamiseks ja vastavuse tagamiseks annab Euroopa Andmekaitsenõukogu välja erinevaid andmekaitse valdkonna teemasid puudutavaid suunised, soovitusi ning jagab parimaid tavasid.[17]

Isikuandmetena käsitletakse üldmääruse kohaselt igasugust teavet tuvastatud või tuvastatava

tagamiseks (vt nt NIS2 pp 104: "Üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste osutajad peaksid rakendama sisseprojekteeritud ja vaiketurvet ning teavitama teenuse kasutajaid olulistest küberohtudest ning meetmetest, mida viimased saavad oma seadmete ja side turvalisuse kaitseks võtta, kasutades näiteks teatavat liiki tarkvara või krüpteerimistehnoloogiaid.".).

[13] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

[14] Euroopa rahvastiku- ja eluasemestatistika määruse ettepaneku artiklis 13(2) mainitakse mõistet "füüsilised ja loogilised kaitsemeetmed". Artiklis 13(3)(b) viidatakse "eraelu puutumatust soodustavatele tehnoloogiatele, mis on spetsiaalselt välja töötatud määruste (EL) 2016/679 ja (EL) 2018/1725 põhimõtete rakendamiseks, võttes eelkõige arvesse eesmärgikohasuse, võimalikult väheste andmete kogumise, säilitusaja piiramise, tervikluse ja konfidentsiaalsuse põhimõtteid". Lisaks on sama määruse ettepaneku artiklis 13(4) nimetatud asjaomaseid prooviuuringuid, mille abil Euroopa Komisjon (Eurostat) ja liikmesriigid kontrollivad asjakohaste eraelu puutumatust soodustavate tehnoloogiate sobivust andmete jagamiseks (vt ka sama määruse ettepaneku artiklit 14(1)(e)). Sellised sõnastusettepanekud võivad olla Euroopa Liidu seadusandluses teerajajaks ning seeläbi võib eeldada, et PET-ide kui täiendavate kaitsemeetmete nimetamine tulevastes õigusaktides võib kujuneda heaks tavaks.

[15] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, p 3, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. IKÜMi põhjenduspunkti (edaspidi pp) 1 kohaselt on füüsiliste isikute kaitse isikuandmete töötlemisel põhiõigus. IKÜM-iga sätestatakse õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel ja isikuandmete vaba liikumist ning sellega kaitstakse füüsiliste isikute põhiõigusi ja -vabadusi, eriti nende õigust isikuandmete kaitsele (IKÜM artikkel 1 lõiked 1 ja 2).

[16] Euroopa Andmekaitsenõukogu, Suunised 3/2018 isikuandmete kaitse üldmääruse territoriaalse kohaldamisala kohta (artikkel 3). Versioon 2.1. 12. november 2019. - Internetis kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/EU_suunised/edpb_guidelines_3_2018_territorial_scope_after_consultation_et.pdf (Viimati külastatud 01.03.2023).

[17] Vt Euroopa Andmekaitsenõukogu, Isikuandmete kaitse üldmäärus: suunised, soovitused, parimad tavad, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_et.

füüsilise isiku, andmesubjekti, kohta. Lisaks on täpsustatud, et tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (IKÜM artikkel 4 punkt 1). Isikuandmete töötlemiseks loetakse isikuandmete või nende kogumitega tehtavaid automatiseeritud või automatiseerimata toiminguid või toimingute kogumit, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine (IKÜM art 4 punkt 2).

Oluline on, et isikuandmete töötlemine lähtuks asjaomastest põhimõtetest, mis on sätestatud IKÜMi artikli 5 lõigetes 1 ja 2. Näitena võib tuua usaldusväärsuse ja konfidentsiaalsuse põhimõtte, mille kohaselt tohib isikuandmeid töödelda viisil, mis tagab isikuandmete turvalisuse, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid (IKÜM artikkel 5(1)(f)). Lisaks peab andmetöötlus olema ka seaduslik. Isikuandmete töötlemine on seaduslik ainult juhul, kui selleks on olemas õiguslik alus (vt IKÜM, artikkel 6).

IKÜMi kohaselt peab isikuandmete töötleja võtma kasutusele tehnilised ja korralduslikud kaitsemeetmed, et tagada isikuandmete kaitse (vt IKÜMi artikli 32 nõudeid töötlemise turvalisuse kohta). Üheks võimaluseks on rakendada erinevaid privaatsuskaitse tehnoloogiaid. Kuigi üldmäärus PET-ide kohta nõudeid otsesõnu ei kehtesta, on näiteks isikuandmete pseudonüümimine ja krüpteerimine toodud välja artikli 32(1) punktis a kui asjakohased tehnilised meetmed, millega on võimalik isikuandmeid kaitsta. Samuti on mainitud andmete anonüümimismeetod IKÜMi pp-s 26, mis üldmääruse kriteeriumile vastates võimaldab andmekaitsepõhimõtete mittejärgmist. Selliste tehnoloogiate kasutamise eesmärk on käsitleda võimalikke privaatsusrünnakuid ja hinnata organisatsiooni valduses oleva teabega seotud riske [8]. Samas on oluline, et ka organisatsiooni töötajad oleksid teadlikud isikuandmete töötlemisele kehtivatest nõuetest ja oskaksid neid teadmisi praktikas rakendada. Organisatsioon peab olema vajadusel suuteline tõestama, et ta on sellised meetmed rakendanud. Lisaks on oluline tähele panna, et iga tehnilise kaitsemeetme kasutamine ei pruugi vastata õigusakti nõuetele.

Tehnilised ja korralduslikud meetmed võivad hõlmata näiteks (a) isikuandmete pseudonümimist ja krüpteerimist; (b) isikuandmeid töötlevate süsteemide ja teenuste kestva konfidentsiaalsuse, tervikluse, kättesaadavuse ja vastupidavuse tagamise võimet; (c) füüsilise või tehnilise vahejuhtumi korral isikuandmetele õigeaegse kättesaadavuse ja juurdepääsu taastamise võimet; aga ka (d) tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise korda (IKÜM art 32(1) p-d a-d). Lisaks, vajaliku turvalisuse taseme hindamisel võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, sh edastatavate, salvestatavate või muul viisil töödeldavate isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu (IKÜM art 32(2)).

Sellised regulatiivsed lähenemisviisid peaksid olema tehnoloogianeutraalsed ja paindlikud, võimaldades organisatsioonidel esiteks, rakendada mitmesuguseid privaatsuskaitse tehnoloogiaid ja meetmeid, mis võtavad arvesse konkreetse organisatsiooni spetsiifikaid ja vajadusi; teiseks, arvestada parimaid praktikaid ja tavasid; ning kolmandaks, käsitleda mitmesuguseid privaatsusega seonduvaid ohtusid. Teisest küljest vaadates võivad konkreetsete künniste ja üksikasjalike juhiste puudumine ning õigusaktide tõlgendamise paindlikkus tekitada ebakindlust ja *ad hoc* heuristlikke protsesse. Selline ebakindlus võib omakorda takistada uute tehnoloogiate kasutuselevõttu, mis sõltuvad ühemõttelistest privaatsusnõuetest. Samuti võib see panna organisatsioonid rakendama meetmeid, mis ei suuda tagada piisavat andmekaitse taset [8]. Igal juhul

tuleks andmekaitse põhimõtteid kohaldada igasuguse teabe suhtes, mis puudutab tuvastatud või tuvastatavat füüsilist isikut (IKÜM, pp 26). Seega PET-ide puhul, mida rakendatakse seoses isikuandmete kaitsmisega, tuleks alati järgida ka isikuandmete kaitse nõudeid.

Kuigi IKÜM on otsekohalduv õigusakt, on liikmesriikidel teatud küsimuste otsustamiseks kaalutlusõigus. Eestis on valikukohad sätestatud isikuandmete kaitse seaduses ja eriküsimused konkreetset valdkonda reguleerivates õigusaktides, nt terviseandmetega seotud isikuandmete töötlemise erisused on sätestatud tervishoiuteenuste korraldamise seaduses[18] Ka Eestis võib mitmeid selliseid erisätteid kohata. Näiteks on panganduses kesksel kohal pangasaladuse instituut (vt krediidiasutuste seadus (KAS), § 88), kuivõrd panga ja kliendi vahelised tehingulised suhted põhinevad suuresti pooltevahelisel usaldusel. Pangasaladus on seotud isiku põhiõigustega ja selle avaldamise kohustus saab krediidiasutusele tuleneda üksnes seadusest, poolte vastavast kokkuleppest või kui pank on kohustatud muudel põhjustel kõnealuse saladuse kaitsmise kohustusest loobuma [9].

Samuti on kehtestatud isikuandmete töötlemise eriregulatsioon tervishoiuteenuste korraldamise seaduse (TTKS) alusel, mis võimaldab tervishoiuteenuse osutajal, kellel on seadusest tulenev saladuse hoidmise kohustus, andmesubjekti nõusolekuta töödelda tervishoiuteenuse osutamiseks vajalikke isikuandmeid, sh eriliiki isikuandmeid (§ 4^1 lõige 1). Samuti on sätestatud normid haiglas viibiva andmesubjekti terviseseisundit kajastavate andmete edastamise või nendele juurdepääsu võimaldamisele (§ 4^1 lg 2) ning selgelt reguleeritud terviseandmete dokumenteerimine ja säilitamine (§ 4^2). Isikuandmete kaitse seadus (IKS) reguleerib füüsiliste isikute kaitset isikuandmete töötlemisel ulatuses, milles see täpsustab ja täiendab sätteid, mis sisalduvad IKÜMis (vt IKS § 1 lõige 1 punkt 1). IKS loob üldised raamid isikuandmete töötlemisele, milles Eestil on üldmäärusest tulenev diskretsioon.

IKS-iga on üle võetud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680 (õiguskaitsedirektiiv)[19] nõuded, mistõttu reguleerib IKS ka füüsiliste isikute kaitset isikuandmete töötlemisel õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel ja menetlemisel ning karistuste täideviimisel (IKS § 1 lõige 1 punkt 2). Sellised pädevad asutused on avaliku sektori asutused, näiteks õigusasutused, politsei ja teised õiguskaitseasutused (õiguskaitsedirektiiv, pp 11). Silmas tuleb pidada, et kui viidatud pädev asutus või üksus töötleb isikuandmeid muul eesmärgil kui õiguskaitsedirektiivi kohaselt ette nähtud, kohaldatakse isikuandmete töötlemisele IKÜMi nõudeid (õiguskaitsedirektiiv, pp 34).

Avaliku sektoriga on seotud ka Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist[20]. Viidatud määruse pp-i 48 kohaselt eeldab füüsiliste isikute õiguste ja vabaduste kaitsmine isikuandmete töötlemisel asjakohaste tehniliste ja korralduslike meetmete võtmist ning lõimitud ja vaikimisi andmekaitse põhimõtetele vastavate siseeeskirjade ja meetmete rakendamist. Täpsustatud on, et sellised meetmed võivad koosneda mh isikuandmete töötlemise miinimumini viimisest, isikuandmete võimalikult kiirest pseudonüümimi-

[18] Üksikisikuid puudutavate andmete töötlemine kätkeb endas privaatsusriske ning neid riske on õigus- ja arvutiteaduse valdkondades erinevalt kontseptualiseeritud. Mitmed teabe privaatsust käsitlevad õigusaktid võtavad üle privaatsusriski mõisted, mis on sektori- või kontekstispetsiifilised, nt seadused, mis kaitsevad teatud tüüpi finantsteavet või terviseinfot [8].

[19] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.

[20] Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1725, 23. oktoober 2018, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ.

sest, läbipaistvusest seoses isikuandmete eesmärgi ja töötlemisega, andmesubjektile andmete töötlemise jälgimise võimaluse andmisest ning vastutavale töötlejale võimaluse andmisest luua ja parandada turvameetmeid (määrus (EL) 2018/1725, pp 48). Samuti on lisatud, et lõimitud ja vaikimisi andmekaitse põhimõtteid tuleks arvesse võtta ka riigihangete kontekstis (määrus (EL) 2018/1725, pp 48).

Euroopa Komisjon tegi 2017. a ettepaneku kehtestada privaatsust ja elektroonilist sidet käsitlev määrus[21], millega soovitakse kehtestada ka andmekaitse erinõuded elektroonilise side valdkonnas.[22] Euroopa Andmekaitsenõukogu näeb vajadust kavandatavas määruses rõhutada anonüümimise rolli kui peamist tagatist, mida tuleks elektroonilise side andmete kasutamisel süstemaatiliselt eelistada.[23]

Euroopa Liidu tasemel on kehtestatud ka mitmeid küberturvalisusega seotud õigusakte, mis panustavad samuti privaatsus- ja andmekaitsesse, nt direktiiv 2016/1148 (NIS direktiiv)[24], direktiiv (EL) 2022/2555 (küberturvalisuse 2. direktiiv (NIS 2))[25], määrus (EL) 2019/881 (küberturvalisuse määrus)[26], määrus (EL) 2022/2554 (DORA)[27], määrus (EL) 2021/887[28].[29] Küberturvalisuse meetmete rakendamine mitte üksnes ei taga turvalisust, vaid võib suurendada ka inimeste usaldust digitaalsete teenuste osas.

[21]Ettepanek: Euroopa Parlamendi ja nõukogu määrus milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus), Brüssel,10.1.2017, COM(2017) 10 final, 2017/0003(COD), https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010.

[22]Privaatsust ja elektroonilist sidet käsitleva määruse ettepaneku seletuskirja punktis 1.2. on kirjutatud, et viidatud "ettepaneku puhul on tegemist isikuandmete kaitse üldmääruse suhtes eriõigusaktiga (lex specialis) ning sellega täpsustatakse ja täiendatakse nimetatud määrust isikuandmetena käsitatavate elektroonilise side andmete osas. Kõiki isikuandmete töötlemisega seotud küsimusi, mida ei ole ettepanekus konkreetselt käsitletud, reguleerib IKÜM. Isikuandmete kaitse üldmäärusega vastavusse viimise tulemusena tunnistati kehtetuks teatavad sätted, näiteks e-privaatsuse direktiivi artiklis 4 sätestatud turvalisusega seotud kohustused."

[23]Euroopa Andmekaitsenõukogu, Avaldus 03/2021 e-privaatsuse määruse kohta, vastu võetud 9. märtsil 2021, lk 2, https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_et.pdf (Viimati külastatud 21.01.2023).

[24]Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus

[25]Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, 14. detsember 2022, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv).

[26]Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881, 17. aprill 2019, mis käsitleb ENISAt ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (EMPs kohaldatav tekst). ENISA üks ülesannetest on toetada liikmesriike küberturvalisuse alase teadlikkuse parandamisega, hõlbustades liikmesriikide vahel tihedamat koordineerimist ja parimate tavade vahetamist. ENISA veebilehel (enisa.europa.eu) on võimalik leida erinevaid ülevaateid, nt ajakohaseid ohupilte, ja soovitusi küberturvalisuse valdkonnas. ENISA on hiljuti avaldanud krüptograafia valdkonnas kaks dokumenti: Post-kvantkrüptograafia – integratsiooniuuring (ingl Post-Quantum Cryptography - Integration study) Post-kvantkrüptograafia: praegune seis ja kvantide leevendamine (ingl Post-Quantum Cryptography: Current state and quantum mitigation)

[27]Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, 14. detsember 2022, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011.

[28]Euroopa Parlamendi ja nõukogu määrus (EL) 2021/887, 20. mai 2021, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik.

[29]Vt ka Euroopa Parlamendi ja nõukogu määruse ettepanekut, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020. https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52022PC0454&qid=1679903559124&from=EN. Kavandatava määruse eesmärgiks on kehtestada turvaliste digielemente sisaldavate toodete väljatöötamise tingimused, mis tagaksid, et turule lastavatel riist- ja tarkvaratoodetel oleks vähem nõrkusi ning et kasutajad oleksid selliste toodete küberturvalisusega seotud aspektidest paremini informeeritud (ettepaneku pp-d 1 ja 2).

Näiteks DORA artiklis 9(1) on nimetatud, et finantssektori ettevõtjad peavad IKT-süsteemide ja -vahendite turvalisuse ja toimimise tagamiseks võtma kasutusele asjakohased IKT turvalisuse vahendid, põhimõtted ja menetlused. Turvalised IKT-süsteemid ja -vahendid võimaldavad paremini kaitsta töödeldavaid andmeid, olgu selleks isikuandmed, ärisaladus või muu info.

Euroopa Liidu Küberturvalisuse Ameti (ENISA) üheks ülesandeks on tutvustada ka mitmetegurilise autentimise, paikamise, krüptimise, andmete anonüümseks muutmise ja andmekaitse alaseid nõuandeid (NIS2 pp 40), mis suurendab teadlikkust ühiskonnas erinevate kaitsemeetmete osas.[30]

> *"Liikmesriigid peaksid ergutama uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamist, mis võiks parandada küberrünnete avastamist ja ennetamist ning ressursse küberrünnete vastu paremini suunata. Seepärast peaksid liikmesriigid sellise tehnoloogia kasutamise hõlbustamiseks soodustama oma riiklikes küberturvalisuse strateegiates teadus- ja arendustegevust, eelkõige seoses küberturvalisuse automatiseeritud või poolautomaatsete vahenditega, ning, kui see on kohane, jagama sellise tehnoloogia kasutajate koolitamiseks ja tehnoloogia täiustamiseks vajalikke andmeid. Uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamine peaks olema kooskõlas liidu andmekaitseõigusega, sealhulgas andmekaitsepõhimõtetega, nagu andmete täpsus, võimalikult väheste andmete kogumine, õiglus ja läbipaistvus ning andmeturve, näiteks tipptasemel krüpteerimine. Määruses (EL) 2016/679 sätestatud lõimitud ja vaikimisi andmekaitse nõuetest tuleb täielikult kinni pidada."* (NIS2 pp 51)

Tehisintellektiga seonduvate riskide leevendamiseks on EL astunud seadusandlikke samme. 2021. aastal esitati tehisintellekti käsitleva määruse ettepanek[31], mille eesmärgiks on soodustada tehisintellekti kasutuselevõttu ja leevendada seotud riske (ettepaneku seletuskiri, p 1.1.). 2022. aastal järgnes tehisintellektiga seotud vastutuse direktiivi ettepanek[32], millega soovitakse tagada, et tehisintellekti põhjustatud kahju kandnud isikud saaksid mõistlikult oma õiguseid kaitsta. Selleks ühtlustatakse riiklikke lepinguvälise süülise vastutuse norme. Samuti soovitakse tagada suurem õiguskindlus ettevõtjate jaoks, kes arendavad või kasutavad tehisintellekti (ettepaneku seletuskiri, p 1.).

Krüpteerimist, mis on üks privaatsuskaitse tehnoloogiatest, on selgesõnalise võimalusena nimetatud mitmetes EL õigusaktides. NIS2 direktiivi pp-s 98 on isegi mindud kaugemale, selgitades, et vajaduse korral peaks üldkasutatavate elektroonilise side võrkude pakkujatele või üldkasutatavate elektroonilise side teenuste osutajatele olema käesoleva direktiivi kohaldamisel

[30] NIS 2 direktiivi pp 98 kohaselt tuleks üldkasutatavate elektroonilise side võrkude ja teenuste turvalisuse tagamiseks "edendada krüpteerimistehnoloogiate kasutamist, eelkõige otspunktkrüpteerimist ja andmekeskseid turbekontseptsioone, nagu kartograafia, segmenteerimine, märgistamine, juurdepääsupoliitika ja juurdepääsu haldamine ning automatiseeritud juurdepääsu otsused. Vajaduse korral peaks üldkasutatavate elektroonilise side võrkude pakkujatele või üldkasutatavate elektroonilise side teenuste osutajatele olema käesoleva direktiivi kohaldamisel kohustuslik kasutada krüpteerimist, eelkõige otspunktkrüpteerimist, kooskõlas turbe ja privaatsuse vaikesätteid ja sisseprojekteerimist käsitlevate põhimõtetega. Otspunktkrüpteerimise kasutamine tuleks ühildada liikmesriikide volitustega tagada nende oluliste julgeolekuhuvide ja avaliku julgeoleku kaitse ning võimaldada kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist kooskõlas liidu õigusega. Sellega ei tohiks aga kaasneda otspunktkrüpteerimise nõrgestamine, kuna see on tõhusa andmekaitse, privaatsuse ja side turvalisuse jaoks olulise tähtsusega tehnoloogia".

[31] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52021PC0206.

[32] Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv lepinguvälise tsiviilvastutuse normide tehisintellektile kohandamise kohta (tehisintellektiga seotud vastutuse direktiiv). https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52022PC0496&from=EN

kohustuslik kasutada krüpteerimist, eelkõige otspunktkrüpteerimist, kooskõlas turbe ja privaatsuse vaikesätteid ja sisseprojekteerimist käsitlevate põhimõtetega. Isikuandmete krüpteerimist peetakse laialdaselt privaatsust säilitavaks tehnoloogiaks, millel võib olla võtmeroll uuendusliku IT-tehnoloogia vastavuses Euroopa andmekaitseõiguse raamistikule [10]. Krüpteeritud andmetel on andmesubjektide privaatsuse kaitsel oluline roll. Selle õiguslikud probleemid on tihedalt seotud andmekaitseseaduste kohaldamisala ning pseudonüümimise ja anonüümseks muutmise õiguslike tagajärgedega [10].

On väidetud, et olukorras, kus kasvõi ühel inimesel on juurdepääs andmete dekrüpteerimise võtmele, anonüümseid andmeid ei eksisteeri. Alternatiivne seisukoht on see, et kui vastutav andmetöötleja annab krüptitud andmed kolmandale osapoolele töötlemiseks ilma krüpteerimisvõtmeta, on sellel kolmandal isikul anonüümsed andmed. Näitena on toodud, et kui keegi edastab ajakohase ja piisava krüpteeringuga kaitstud andmed niiöelda mustas kastis, siis võib eeldada, et mõistlikke vahendeid kasutades ei ole andmetöötlejal võimalik suletud mustas kastis olevaid andmeid töödelda [11].

Krüpteerimine võib olla füüsilise isiku privaatsuse kaitsmise võti ja teha võimalikuks mitmed IT-uuendused, mis muidu oleksid vastuolus privaatsus- ja andmekaitse nõuetega. Näiteks valdkondades, mis puudutavad terviseandmete töötlemist, asjade internetti, suurandmeid või pilvtöötlustehnoloogiaid. Kuna andmed võivad arvutamise ajal jääda krüpteerituks, võivad need andmed jääda krüpteerituks ka analüütilistes keskkondades, nii et andmed on varguse või väärkasutuse suhtes kaitstud isikustamise rünnete eest [6].

Privaatsuskaitse ja küberturbe tehnoloogiatega on puutumuses ka andmekogudega seotud küsimused, eeskätt, kuidas töödelda andmekogu(de)s olevaid andmeid selliselt, et andmesubjekti õiguste riive oleks minimaalseim, tema andmed oleksid kaitstud ja õigused tagatud. Avaliku teabe seadus defineerib andmekogu mõiste. Selle § 43[1] lõike 1 kohaselt on andmekogu riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks. Andmekogus töödeldavate korrastatud andmete kogum võib koosneda ka üksnes teistes andmekogudes sisalduvatest unikaalsetest andmetest (AvTS § 43[1] lõige 2) ja andmekogusse andmete kogumisel lähtutakse andmete ühekordse küsimise põhimõttest (AvTS § 43[1] lõige 3).

Andmete ühekordse küsimise põhimõtte rakendamine vähendab andmete esitajate halduskoormust aga tagab ka riigi tõhusama toimimise. Kui organisatsioonil on temale seadusega või seaduse alusel antud ülesannete täitmiseks vaja töödelda andmeid, mis on juba ühes andmekogus olemas, siis ei tohiks neid enam täiendavalt küsida ja olemasolevaid andmeid tuleks n-ö taaskasutada[33], kui vastavat õigust ei ole eriseadustega piiratud.

Erinevate andmekogude andmete ühildamise temaatika viib ühtlasi suurandmete (massandmete) töötlemisega seotud teemadeni. Üha enam soovivad organisatsioonid ja ettevõtted kasutada suurandmetel põhinevat andmetöötlust ja analüütikat. Seda soosib ka Euroopa Liit[34]. Riigikant-

[33] Eelneva teemaga seonduvad ka andmelaod, millele ei ole kehtestaud eraldiseisvat õiguslikku regulatsiooni. Andmekaitse Inspektsiooni poolt läbiviidud seire ühe järeldusena soovitatakse andmelao testimiseks kasutada sünteetilisi andmeid või hägustatud (obfuskeeritud) andmeid. Ühe lahendusena, mis vähendaks riske, soovitatakse kasutada ka virtuaalset andmeladu, kus ei koondata andmeid ühte kokku, vaid see lahendatakse andmepäringute kihina. Allikas: Andmekaitse Inspektsioon, Andmeladude seire kokkuvõte. – Internetis kättesaadav: https://www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf (Viimati külastatud 02.03.2023).

[34] Vt nt andmehalduse määruse pp 6 ja avaliku teabe laiema taaskasutamise soovi kohta – Euroopa Ülemkogu, Andmejagamise edendamine: eesistujariik saavutas Euroopa Parlamendiga kokkuleppe andmehalduse määruse suhtes (30.11.2021). - Internetis kät-

selei on kirjutanud, et avalik sektor ja poliitika kujundajad peavad arvestama laiemalt maailmas toimuvate muutustega, sh vajadusega teha otsuseid järjest kiirenevas tempos, kaasates samaaegselt järjest suuremat hulka ning varieeruvas formaadis andmeid [35].

Suurandmete (ingl k *big data*) mõistet seadusega defineeritud ei ole. Küll aga on suurandmeid käsitletud näiteks väliskaubanduse- ja infotehnoloogiaministri määruses "digitaliseerimise teekaardi toetamise tingimused ja kord", kus suurandmeid ja nende analüütikat loetakse digitaalsetel tehnoloogiatel põhinevaks rakenduseks (§ 3 lõige 1 punkt 4)[36]. Suurandmed on defineeritud ISO/IEC 20546 standardis kui ulatuslikud andmestud, mis eelkõige mahu, mitmekesisuse, kiiruse ja kõikuvuse tõttu nõuavad tõhusaks salvestuseks, käitluseks, halduseks ja analüüsiks mingit mastaabitavat tehnoloogiat. Suurandmed on tavaliste vahendite võimalusi ületavate andmestute populaarne nimetus, mille kvantitatiivne sisu muutub ajas ja kajastab mahtude eksponentsiaalset kasvu[37].

Suurandmete töötlusel põhinevad lahendused võimaldavad muuta protsesse efektiivsemaks erinevates eluvaldkondades. Samas esineb suurandmete töötlemisel mitmeid probleeme, alates andmestike kvaliteedist juriidiliste küsimusteni. Suurandmete töötlemisel on leitud, et asjaomane Eesti õiguskeskkond ei ole piisav. Näiteks on juba 2016. aastal Andmekaitse Inspektsioonile muret valmistanud korrakaitseseaduses (KorS) massandmetöötluse regulatsiooni puudumine[38].

Leitud on, et KorS § 5 lõige 7 ei ole käsitletav järelevalve otstarbelise massandmetöötluse üldise õigusliku alusena. Lisaks on nenditud, et kui iga organisatsiooni puhul kehtestatakse massandmetöötluseks erimeetmed eriseadustes, vähendab selline olukord õigusselgust ja viib tagasi KorSi eelsesse kirjususse [12]. Andmekogude ja isikuandmete analüüsi (2021) kohaselt on Justiitsministeerium võtnud enda tegevusplaani massandmetöötluse lubatavuse tingimuste analüüsimise, et välja töötada asjakohane õiguslik alus KorSis andmevõrdluseks ohuennetuse faasis [12]. See rehkendus lahendab vaid osa probleemist, kuid on hea suunanäitaja ka teiste sektorite tarbeks.

Ebapiisavat õiguskeskkonda toodi intervjuude käigus välja erinevates valdkondades, mis sooviksid suurandmeid ja seotud andmetöötlust oma igapäevastes protsessides kasutada. Seetõttu võiks seadusandja mõelda universaalsetele nõuetele, mis puudutab suurandmete töötlemist, et tagada õigusselgus ja seeläbi organisatsioonidele ja ettevõtetele teatud kindlustunne, mis käesoleval ajal puudub[39]. Selline olukord võib tekitada EL riikide vahel ka ebavõrdset konkurentsi.

Suurandmete töötluse probleemid ei ole üksnes regulatiivsed. Esineb ka tehnilisi takistusi, nt on Andmekaitse Inspektsioon toonud andmeladude seire kokkuvõttes välja, et X-teel on käesoleval ajal raskusi suurte andmemahtude vahetamisega[40], kuivõrd X-tee on loodud ja toimiv pigem

tesaadav: https://www.consilium.europa.eu/et/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/ (Viimati külastatud 02.03.2023).

[35] Riigikantselei, Andmepõhine otsustamine, https://www.riigikantselei.ee/valitsuse-too-planeerimine-ja-korraldamine/valitsuse-too-toetamine/andmepohine-otsustamine (Viimati külastatud 27.02.2023).

[36] Samuti käsitletakse suurandmeid koos analüütikaga ettevõtlus- ja infotehnoloogiaministri määruses "ettevõtte digipöörde toetuse tingimused ja kord"digitaalsete tehnoloogiate rakenduse kontekstis (vt § 4 punkt 6).

[37] AKIT, Suurandmed, https://akit.cyber.ee/term/1905-suurandmed (Viimati külatatud 21.01.2023).

[38] Andmekaitse Inspektsioon, Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2016. aastal. Soovitused aastaks 2017. Lk 62. https://aastaraamat.aki.ee/sites/default/files/aastaraamatud/aastaraamat_2016.pdf (Viimati külastatud 02.03.2023).

[39] IKÜMi pp-s 41 on selgitatud, et kui IKÜMis osutatakse õiguslikule alusele või seadusandlikule meetmele, ei pea selleks tingimata olema parlamendi poolt vastu võetud seadusandlik akt.

[40] Andmekaitse Inspektsioon, Andmeladude seire kokkuvõte, Seire järelduse punkt 5. – Internetis kättesaadav: https://www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf (Viimati külasta-

väiksemahuliste päringute ja edastuste korral. Andmevahetuseks on võimalik kasutada ka erinevaid pilvteenuseid, kuid kasutajad põrkuvad siin erinevate andmekaitseliste ja turvanõuetega. Ühe võimalusena oleks võimalik kaaluda riigi poolt keskse turvalise suurandmete vahetamise keskkonna loomist.

2.3 Kokkuvõte

Privaatsus- ja andmekaitse nõuetega tuleb privaatsuskaitse tehnoloogiate rakendamise puhul arvestada eeskätt siis, kui tegemist on isikuandmete töötlemisega. Samas on hästi oluline teadvustada, et nende tehnoloogiatega on võimalik lisaks isikuandmetele kaitsta ka muud teavet, näiteks äri- või riigisaladusi.

Olenevalt jurisidktsioonist võivad olla privaatsus- ja andmekaitsenõuded erinevad. ELis kehtestab viidatud valdkonns peamised nõuded, millega organisatsioon või ettevõte peab arvestama, IKÜM. Kuigi IKÜM on otsekohalduv määrus, siis tuleb arvestada selle direktiivilaadse olemusega, mis võimaldab liikmesriikidel oma seadusandluses ette näha hulga erisusi.

Kui me räägime pseudonüümitud andmetest, siis tuleb IKÜMi norme kohaldada terve andmetöötlusprotsessi vältel, st alates andmete kogumisest kuni nende kustutamiseni. Kui me käsitleme anonüümitud andmeid, siis tulenevalt anonüümimismeetodist ja selle efektiivsusest (taasidentifitseerimise tõenäosuse mõttes) võib IKÜMi normide kohaldumine olla mõnevõrra erinev, sõltudes vastava meetme pakutavast kaitsetasemest. Näiteks saavutades anonüümimismeetoditega andmete sellise olemuse, mille korral ei ole mistahes viisil isiku taastuvastamine võimalik, tuleb tagada, et IKÜMi nõuded on järgitud vähemalt kuni sellise tulemuse saavutamiseni.

Teadus- ja õiguskirjanduses, mis käsitleb privaatsuskaitse tehnoloogiaid, on peamiseks arutluskohaks see, millise taseme võib privaatsuskaitse meetod saavutada, st kas tulemuseks on pseudonüümsed või anonüümsed andmed ning kas see võib sõltuvalt meetodist ja meetodi kasutamise kontekstist erineda. Tulenevalt sellest, kas tegemist on IKÜMi kohaselt pseudonüümsete või anonüümsete andmetega, sõltub ka IKÜMi asjaomaste normide kohaldamine. Lähtuvalt eelnevast oleks väga oluline uurida täiendavalt erinevaid meetodeid, millega oleks võimalik tehnoloogiate privaatsuskaitse taset mõõta ja hinnata.

Tugevaid andmekaitse meetmeid, sealhulgas privaatsuskaitse ning läbipaistvuse ja sekkutavuse tehnoloogiaid nähakse digimajanduse eluspüsimise võtmena. Nendega on võimalik säilitada usaldus riigi vastu, et isiku andmeid töödeldakse turvaliselt ja võimalikult vähese privaatsusriivega. Regulatsioone on võimalik muuta, ja vajadusel tulebki seda teha, samas on seejuures oluline tagada ka isikute põhiõigused. Privaatsuskaitse ning läbipaistvuse ja sekkutavuse tehnoloogiate arendamine ja rakendamine võimaldavad teostada vastutustundlikku andmeinnovatsiooni, mis võiks kokkuvõttes tuua kasu tervele ühiskonnale.

tud 02.03.2023).

3 Eesti kogemused privaatsuskaitse tehnoloogiatega

3.1 Sissejuhatus

Siin peatükis kirjeldame, milliste privaatsuskaitse tehnoloogiatega on Eesti teenuste ja infosüsteemide ehitajatel kogemusi. Info kogusime kokku nii asutustega tehtud intervjuudest kui avalikest allikatest.

Kokkuvõtlikult on kogemusi erineval tasemel: leidub nii välja ehitatud ja juurutatud süsteeme, poolikuid süsteeme kui ka analüüse ja kavatsusi. Mõnede privaatsuskaitse tehnoloogiate puhul on tehtud prototüüpe teadus-arendusprojektide käigus. Alljärgnevalt oleme kogemused struktureerinud selle järgi, mille kaitseks privaatsuskaitse tehnoloogiad rakendatud on.

3.2 Andmete kaitse infosüsteemides ja analüütilisel töötlemisel

Pseudonüümimine. Andmete pseudonüümimisega on kokku puutunud enamik intervjueeritutest ja arvestades tehnoloogia kõrget küpsust võime eeldada, et seda rakendatakse veel paljudes teisteski organisatsioonides. Vahel kutsustatakse seda hägustamiseks või obfuskeerimiseks, kuid ühine joon on otseselt isikustavate tunnuste (näiteks isikukoodide) teisendamine või asendamine.

Uuringut tehes kogesime terminoloogilist segadust pseudonüümimise ning anonüümimise õigusliku ja tehnilise tähenduse vahel, selle teema algatasid sageli intervjueeritavad ise. Mitmed tehnikad, mida nimetatakse anonüümimiseks, võivad saavutada õiguslikus tähenduses (IKÜM põhjenduspunkt 26 mõistes) pseudonüümimise. On alust arvata, et tegemist on Eestis kõige enam kasutust leidnud privaatsuskaitse tehnoloogiaga.

Statistikaamet rakendab pseudonüümimist statistika tootmise protsessis ning selleks on selged majasisesed kokkulepped ja ühtsed juhised.

Eesti Geenivaramus toimub pseudonüümimine spetsiaalses õhkeraldatud kodeerimiskeskuses. Geeniandmed ja haiguslugu kogutakse ja töödeldakse, et eemaldada haigusloost isikustatud informatsioon ning identifikaatorid asendatakse ühekordsete pseudonüümidega. Pseudonüümide pööramiseks vajalik informatsioon talletatakse vaid kodeerimiskeskuses, vastavalt inimgeeniuuringute seadusele.

Pseudonüümimist rakendatakse ka teistes asutustes, näiteks Transpordiametis, Justiitsministeeriumis, Tervisekassas, Sotsiaalministeeriumis, Siseministeeriumi haldusalas ning Tervise ja Heaolu Infosüsteemide Keskuses (TEHIK). Sotsiaalministeeriumil on selleks ka vastav eraldi teenus.

Justiitsministeerium tõi välja, et teadustööde raames, mis hõlmavad mitme erineva vastutava töötleja andmekogusid, pole selge, kes peaks andmed kokku panema. Konkreetsed normid või suunised eelneva osas puuduvad, kuid nende olemasolu tagaks vajaliku (õigus)selguse.

Mitmest intervjuust selgus, et andmebaaside privaatsust säilitava ühendamise probleem on paljudel riigiasutustel ühine ning privaatsuskaitse tehnoloogiad saaksid siin abiks olla.

Riigi Infosüsteemi Amet (RIA) arendab Bürokrati süsteemis keskset klassifitseerimise teenust, mis otsustab, millisele asutusele lõppkasutaja sõnumid edasi suunata. Samas ei ole vaja sel klas-

sifitseerijal teada isikuandmeid ja seega asendatakse need juhuslike väärtustega. RIA arendab ka eestikeelse teksti pseudonüümimise lahendust, mille eesmärk on eemaldada tekstist otseselt isikustavad osad.

Anonüümimine. Sarnaselt pseudonüümimisele on ka anonüümimisega kokku puutunud mitmed intervjueeritutest.

Statistikaamet avaldab oma avaldamiskanalites (välisveeb, väline andmebaas, kliendirakendused) ainult anonüümitud andmed, n-ö avaandmed, mis on kokkuvõtted agregeeritud andmete pealt (anonümimine koondamise teel). See saavutatakse Statistikaametis välja arendatud metoodika abil.

Eesti Maksu- ja Tolliamet (EMTA) kinnitab, et andmete anonüümimine on keerukas. Arendusprojektides on vaja anonüümseid testandmeid, mis aga samal ajal peavad olema piisavalt detailsed, et nende alusel saaks arendada korrektse äriprotsessi ja kontrollida neid ka päriseluga. Äriprotsessi reeglid on keerulised ja eeldavad testandmetelt seoste olemasolu, mistõttu nende loomine on täna käsitöö.

Sama kehtib masinõppemudelite loomise juures, kus päris andmetega ei ole lubatud katsetada. EMTA on kaalunud sünteesitud andmeid ja anonüümimist. Selline töö eeldab andmebaaside struktuuri väga detailset läbivaatust, mis on mahukas käsitöö. Ka Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) kasutab anonüümimist testandmete puhul, kus ei saa anda juurdepääsu päris andmetele. Teine oluline anonüümimise koht SMIT jaoks on andmelaondus ja statistika, kus olulised on arvud, aga mitte see, missugused isikud nende taga on. Politsei- ja Piirivalveamet (PPA) toob kogemustest välja mure, et kui tellitakse väline partner andmeid analüüsima, siis tekib küsimus, et milliseid andmeid saab talle üldse sisendiks anda? Teostades vajaliku anonüümimise võib tulemuseks olla kasutu andmemudel.

Ka Tervisekassa anonüümib andmeid käsitsi. Anonüümimismeetodid on kontekstist lähtuvad, et mõistliku vaevaga ei oleks inimene tuvastatav. Finantsinspektsioon on oma tegevustes anonüümimist kasutusele võtmas.

Piirangutega liidesed. Statistikaametil on koostöö Eesti Pangaga, kus viimane saab läbi spetsiaalse VPN-i ligi kokkulepitud osale andmetest.

Analüütiku töökohad. Välistele osapooltele on hetkel on Statistikaametis kasutusel nii füüsilised ruumid kui teadlase virtuaalne töökeskkond, mis kasutab VPN lahendust ja kuhu soovija autendib end ID-kaardiga (või e-residendi kaardiga). Selles keskkonnas saab kasutada vaid sinna ette valmistatud andmeid ja sealt välja ei saa viia midagi ilma Statistikaameti töötaja abi või järelevalveta. Lähiaastail on plaanis füüsilistest analüüsiruumidest ja praegusest tehnilisest lahendusest loobuda ning asendada see uue keskkonnaga, kus saab ligi kogu Statistikaameti andmekataloogile. See tõstab huvi Statistikaameti andmete vastu ja selle tõttu võib kasvada konfidentsiaalsuskontrollide maht. Tartu Ülikooli Eesti geenivaramu (EGV) on välja ehitamas “andmepuuri” lahendust, et takistada erinevate teaduslikeks eesmärkideks antud andmekogude omavahelist kokku viimist ning muul moel soovimatut töötlemist. EGV plaanib kasutada oma kodeerimiskeskuse lahendust, et andmed teadustööks ette valmistada. Näiteks, seostatakse genotüübiga fenotüübist vaid andmed haiguste, patoloogiate või muude uuritavate tunnuste kohta. Selline andmestik tehakse siis kättesaadavaks eemalt ühenduvale kasutajale selleks ette nähtud taristul. Kui andmepuur tööle hakkab, saab sellest EGV eelistatud lahendus teadlastega koostööks.

Maksu- ja Tolliamet on kasutanud erilahendusi, kus lepingute ja mitmete turvameetmete kombinatsioonis on lubatud andmeteadlaseid analüüsima maksuandmeid.

Diferentsiaalprivaatsus. Eestis on diferentsiaalprivaatsust ja selle tööriistu uuritud teadusuuringutes, kuid intervjuudest ei selgunud, et Eestis seda tehnoloogiat rakendatud oleks.

Liitõpe. Eestis on kogemused liitstatistikaga. Näiteks sideoperaatorid ja Statistikaamet koostasid SARS-COV-2 pandeemia ajal üle mitme operaatori liikuvusstatistika aruande. Sideoperaatorid tegid ära eeltöö enda käsutuse olevate mobiiltelefonide asukohaandmete peal ning edastasid koondtulemused Statistikaametile, kes vormistas nendest üleriigilise aruande.

Liitõpet on Eestis kutsutud ka hajusõppeks. Selle teemal on käimas kiire areng ning planeerimisel on mitmeid lahendusi, sh ka Bürokrati arenduses.

Sünteetilised andmed. Sünteetiliste andmetega, mis oleks automaatselt genereeritud ja mis järgiks aluseks olnud andmekogu statistilisi näitajaid, intervjueeritutel otsest kogemust ei ole. Sellel teemal on Eestis tehtud teadus-arendusprojekte.

TEHIK, RMIT ning Majandus- ja Kommunikatsiooniministeerium räägivad sünteetilistest andmetest infosüsteemide arenduse ja testimise kontekstis, sest päris andmeid selleks otstarbeks kasutada ei tohi. Hetkel koostatakse testimiseks andmekogusid käsitsi ning see on arendussurvet arvestades suur pingutus. Nii loodud testandmete kvaliteeti on keeruline tagada ja seega on siin ka suured võimalused olukorra parendamiseks.

Päästeameti andmete vastu tunnevad huvi lõpu- või magistritööde kirjutajad ning selleks, et katsetada, kas välja pakutud hüpotees peab paika, tuleb neile genereerida näidisandmed. Hetkel teeb Päästeamet seda käsitsi.

Usaldatavad täitmiskeskkonnad. Riigiasutustes rakendusi uuringu intervjuudes välja ei toodud. Eestis on aga tehnoloogiat privaatuse kaitseks rakendatud küll.

Cybernetica AS ja Positium on koostöös välja arendanud demonstraatori, mis analüüsib Eestis rändlevate (*roaming*) mobiiltelefonide liikumist, et pakkuda ajakohast ja täpset sisendit turismiteenuste edendamiseks.[41] Iga mobiiltelefoni liikumisest tekib sideoperaatori juurde jälg, kuid kuna tegemist on delikaatse infoga, pole sideoperaatoril üldjuhul võimalik neid andmeid jagada. Mainitud demonstraator kasutab usaldatavat täitmiskeskkonda ning töötleb mobiilseid asukohaandmeid krüpteeritult. Asukohaandmed krüpteeritakse nende lähtekohas sideoperaatori juures ning krüpteerimisvõti on teenuseandja eest riistvaraliselt kaitstud. Teenus väljastab ainult eelnevalt kokku lepitud agregeeritud andmeid (nt statistika riikide kaupa) ning isegi teenuseandja ei pääse ligi algandmetele, kuigi need on (krüpteeritult) tema hallatavas serveris.

Homomorfne krüptograafia. Uuringu käigus ei leitud kogemusi, et homomorfset krüptograafiat oleks kasutatud andmete töötlemiseks.

Turvaline ühisarvutus. Turvalise ühisarvutuse tehnoloogiat on Eestis rakendatud mitmel korral ning mitmel intervjueeritud riigiasutusel on olnud selles oma roll. 2013. aastal loodi RIA tellimusel

[41] Cyber Security for Europe. D3.13 Updated version of enablers and components. 2021. https://cybersec4europe.eu/our-results/deliverables (viimati külastatud 03.03.2023).

demorakendus, mis näitlikustas turvalise ühisarvutuse tehnoloogia kasutamist, arvutades agregeeritud näitajaid Eesti avaliku sektori palgaandmetel (mis tõsi küll, pole Eestis salajased). Demo esitleti juhtiavale Euroopa pilvandmetöötluse arendamise nõukojale [13]. Kuigi tegemist oli demonstraatoriga, olid arvutusosapooled sõltumatud (SMIT, RIA ja Cybernetica AS) ning ühelgi osapoolel polnud ainuisikulist kontrolli arvutuse üle.

2015. aastal viis CentAR selle tehnoloogia abil läbi uuringu, kus ühendas ülikoolis õppinute haridusandmeid ning samade inimeste maksuandmed [14]. Uuringu eesmärk oli aru saada, kas ja kuidas mõjutab õpingute ajal töötamine tudengite edasisi õpinguid ja karjäärivalikuid. Uuringuks vajalik sisend saadi Haridus- ja Teadusministeeriumist (Eesti Hariduse Infosüsteemist (EHIS)) ja EMTAst. Arvutusosapooli oli kolm: RMIT, RIA ja Cybernetica AS, kusjuures neist esimene teostas ka turvalise ühisarvutuse platvormi koodi läbivaatuse. Aasta hiljem toimus teine turvalisel ühisarvutusel põhinev uuring, kus sisendiks olevad andmekogud olid samad, aga uurimisküsimus oli seotud hariduslike erivajadustega õpilaste arenguvõimalustega [15]. Arvutusserverite majutajateks olid seekord RMIT, HTM ja Cybernetica AS (Zone pilves).

Lisaks intervjueeritutele on turvalise ühiarvutuse tehnoloogiat rakendanud ka Tartu linnavalitsus, kes 2016. aastal viis selle abil läbi rahulolu-uuringu oma enam kui 300 töötaja hulgas [16, 17]. Selliselt korraldatud küsitlus annab potentsiaalselt õigema ülevaate, kuna vastajad saavad olla kindlad, et mitte keegi (ka süsteemi administraator) ei näe nende vastuseid ning tänu sellele julgevad nad ehk olla ausamad. Kõrgendatud privaatsusgarantiidega küsitlussüsteemi juurutamine toimus EL raamprogrammi FP7 projekti PRACTICE raames ning arvutusosapoolteks olid Cybernetica AS Eestist ning projektipartnerid Alexandra Institute ja Partisia Taanist.

3.3 Identiteedi ja tõendustehingute kaitse

Pimesignatuurid. Eestis teadaolevalt rakendatud ei ole.

Rühma- ja ringisignatuurid. Eestis teadaolevalt rakendatud ei ole.

Atribuutkrüptograafia. Eestis teadaolevalt rakendatud ei ole.

Nullteadmustõestused. Nullteadmustõestuseid kasutatakse Eestis e-hääletuse süsteemis kahes kohas – miksimistõendi ja lugemistõendi juures. Lugemistõend on realiseeritud Schnorri nullteadmustõestusel põhineval protokollil. Miksimistõendis on kasutatud Verificatumi miksimissüsteemiga seotud nullteadmustõestust [18, 19].

3.4 Anonüümne side ja tehingud

Turvaline vestlus. Otspunktkrüpteeritud vestlusrakenduste kasutamist intervjueeritavad ei maininud. Mitteametlikult ja töötajate endi entusiasmist on aga Signal ja selle protokollil põhinevad vestlusrakendused (nt WhatsApp) kasutusel vähemalt PPAs [20].

RIA hallatava Bürokrati sõnumivahetuses on kavandatud otspunktkrüpteeringu kasutamist.

Mikservõrgud. Eesti e-hääletuse süsteemi arendatakse iga kasutuskorraga järjest edasi. Alates 2017. aastast kasutusel olev IVXV arhitektuur kastab häälte kokkulugemise etapis allkirjastatud e-häälte anonüümimiseks mikservõrke. Lisaks anonüümitud häältele väljastab see mikservõrk

ka nullteadmustõestuse korrektsuse kohta[42], mille abil saavad välised audiitorid veenduda, et protsessi käigus hääli sisuliselt ei lisata, kustutata ega muudeta.

Sibulmarsruutimine. Sibulmarsruutimise kasutamise kohta Eesti avalikus sektoris infot ei ole. Sibulmarsruutimise platvormi Tor mõõdikute järgi on Eestis üle tuhande igapäevase kasutaja.

3.5 Läbipaistvust ja sekkutavust toetavad tehnoloogiad

RIA pakub kahte läbipaistvuse ja sekkutavuse teenust, milleks on andmejälgija ja nõusolekuteenus. Andmejälgija [43] kogub X-tee teenustest ning infosüsteemidest isikustatud toimingute infot ning näitab seda autenditud kasutajale. Teenuse abil on võimalik näha, kuidas on riigiasutused isiku andmeid kasutanud. Tegemist on teenusega, millel on kõrge küpsusaste ning mida esitletakse Eesti e-riigi läbipaistvuse ühe põhilise meetmena.

RIA on arendamas nõusolekuteenust[44], mille abil saab isik anda riigile loa jagada tema isikuandmeid kindla teenuseandjaga. Võimalik on nõusolek ka tagasi võtta.

Eesti Geenivaramu on välja töötamas doonoriportaali teenust, mis annab doonoritele võimaluse tutvuda enda andmetega ning nende töötlemisega. Muuhulgas saab doonor tulevikus näha ka informatsiooni teadusuuringute kohta, milles tema andmeid on kasutatud.

[42] Verificatum AB. User Manual for the Verificatum Mix-Net. VMN Version 3.1.0. 2022. https://www.verificatum.org/files/vmnum-3.1.0.pdf (viimati külastatud 01.03.2023)

[43] Inimkeskne andmehaldus. Andmejälgija. Riigi Infosüsteemi Amet. https://ria.ee/riigi-infosusteem/inimkeskne-andmehaldus/andmejalgija(viimati külastatud 01.03.2023).

[44] Inimkeskne andmehaldus. Nõusolekuteenus. Riigi Infosüsteemi Amet. https://ria.ee/riigi-infosusteem/inimkeskne-andmehaldus/nousolekuteenus (viimati külastatud 01.03.2023).

4 Eesti riigiasutuste privaatsuskaitse-alased vajadused

Raporti koostamiseks läbiviidud intervjuude käigus paluti intervjueeritud organisatsioonide esindajatel muuhulgas kirjeldada organisatsiooni vajadusi ja väljakutseid, mille lahendamisele privaatsustehnoloogiad otseselt või kaudselt kaasa võiksid aidata. Allpool on lühikokkuvõtted iga organisatsiooni vajaduste kohta esitatud tähestikulises järjekorras.

4.1 Andmekaitse Inspektsioon

Andmekaitse Inspektsioonil endal otsene vajadus privaatsuskaitse tehnoloogiate järele puudub, ent tänu pöördumistele näevad nad teiste asutuste vajadusi. Sellest tulenevalt hindavad Eesti kontekstis olulisimaks järgmiseid PETide võimalikke kasutuskohtasid arendustegevustes:

- Tehisintellekti treenimine: sünteetiliste, mitte pärisandmete abil.
- Andmete ühte kohta kogumisest hoidumine, eelistada hajusalt kasutamist.
- Andmekogude loomisel/infosüsteemide arendamisel testandmete kasutamine.
- Võimaluste loomine sellistele teadusuuringutele, kus väga täpse hüpoteesita soovitakse ligipääsu paljudele andmestikele lootuses neist midagi avastada.

4.2 Eesti Geenivaramu

Geeniandmete eripära on, et referentsmaterjali olemasolul on nende anonümimine põhimõtteliselt võimatu. Seetõttu on privaatsuskaitse tehnoloogiate rakendamine geeniandmete töötlemiseks äärmiselt oluline.

Geenivaramu soovib privaatsuskaitse tehnoloogiaid rakendada oma analüütiku töökohtades – andmepuuris. Andmepuur takistab teadustöös geeniandmete kokku viimist teiste andmemassiividega ning tekitab andmetöötluse kohta auditeeritava logi. Süsteem on 2023. aasta alguse seisuga rajamisel.

Rahvusvahelise koostöö jaoks näeb Geenivaramu potentsiaali ka liitõppes, millega saaks teha uuringuid, milles iga biopanga, haigla või muu teadusasutuse andmed jäävad tema juurde, kuid analüüsitulemused katavad kõiki andmekogusid.

4.3 Eesti Maksu- ja Tolliamet ning Rahandusministeeriumi Infotehnoloogiakeskus

EMTA kiireloomulised vajadused on seotud infosüsteemide testimisega. Testimiseks kasutatakse võimalikult anonüümseid andmeid. Praegu anonüümitakse andmed käsitsi, et tagada privaatsus, korrektsus ja kasutatavus. See annab ühelt poolt võimaluse infosüstemide arendamiseks ja testimiseks, teiselt poolt tagab võimaluse neid päriselus kontrollida.

EMTA näeb tulevikus vajadust analüütika ja masinõppe rakendamiseks. On vajadus süsteeme õpetada ja kaasata rohkem andmeid, aga mitte isikustatuna, vaid üldistatuna, mis tingib välistest allikatest andmete kaasamise ja liidestamise küsimuse. Uurimis- ja teadustööks tuleb leida nii õiguslikud kui tehnilised lahendused. Samuti kaasneb masinõppe juurutamise sooviga välis-

ekspertide kaasamise probleem. Selge vajadus standardite järele, millistele omadustele peavad vastama sünteesitud ja anonüümitud andmed, et neid võiks pidada anonüümseks.

Teisese kasutusega on seotud ka regulatoorsed piirangud. Riskide ja skooride arvutamine on väga selge ja sihtotstarbeline tegevus, mis on reglementeeritud ja protsessidega kirjeldatud. Teistest andmekogudest või muudest andmebaasidest pärit andmete kasutamisel on pidevalt õhus küsimus, kas neid tohib EMTA andmetega liita ja kas sellest tekib uus andmekooslus.

4.4 Finantsinspektsioon

Finantssektori andmeanalüütika vajadused seostuvad piiriülese järelvalvega. EL liikmesriikide kohalikud järelvalveasutused saadavad andmed EL ühistele järelvalveasutustele, mis annavad märku riskidest, mida kohalikud asutused kontrollida saavad. See pole andmelekete riski tõttu teostatav ilma kõrgemal tasemel privaatsuskaitse tehnoloogiate rakendamiseta. Need tehnoloogiad võiksid anda väga efektiivse lahenduse, mida pole aga põhjust igasse liikmesriiki ehitama hakata, vaid seda tuleks teha keskselt — näiteks Single Supervisory Mechanism (SSM) juures.

Finantsjärelvalve subjekte võiks privaatsuskaitse tehnoloogiad huvitada avatud rahanduse (ing k *open finance*) temaatikas, mis on Euroopa Komisjoni suur eesmärk digitaalse rahanduse strateegias. See eeldab andmete liikumist finantssektori osapoolte vahel, võimaldamaks finantsteenuse osutajate vahelist andmevahetust uute klientide kohta.

4.5 Justiitsministeerium

Justiitsministeerium on AvTSi mõttes vastutav töötleja mitmele infosüsteemile. Nende andmebaaside avaldamine testimiseks ja teadustööks on alati olnud küsimus. Paljude seostega andmebaasid, mida ei saa lihtsalt taasluua, kontrollimaks, kas loodav süsteem toimib. Vaja on tehnoloogiat, mis võimaldaks andmetest identifitseerivad osad välja noppida ja need anonüümida.

Anonüümitavate kohtuandmestike avaldamise plaani pidurdavad ebaselged reeglid, kust jooksevad anonüümimise ja pseudonüümimise piirid õiguslikus mõttes. Vaja on juhiseid, millal oleks andmete agregeerimise tase piisav, et andmed oleksid anonüümitud.

Teadustöö raames pole selget korda, kes peaks mitme erineva vastutava töötleja puhul andmeid kokku panema. Vaja on lahendust, mis võimaldaks andmeid statistika, poliitikaanalüüsi või teadustöö eesmärgil ühendada. Samas on andmete koondamisest tekkiv privaatsusrisk tunnetuslikult suur. Seetõttu peavad olema selged ja jõustatavad reeglid, mis kehtivad andmete töötlemise eesmärgil ühendatud andmekogude kohta ning selle kohta, kui töötlemine lõpetatakse.

Poliitikaanalüüsi ja kriminaalpoliitika valdkonnas tehakse uuringuid ja analüüse, mis tihti hõlmavad teistest andmekogudest andmete kaasamist. Tänane protsess selliste uuringute tegemiseks vajab, sõltuvalt uuringust, vastavat eetikakomiteed ning ka Andmekaitse inspektsiooni luba. Kui privaatsuskaitse tehnoloogiate rakendamine neid protsesse lihtsustaks ja kiirendaks, oleks osapooltel suurem motivatsioon tehnoloogiate rakendamiseks ning privaatsuseesmärkide suunas töötamiseks.

Õigusvaldkonnas on üks unikaalne probleem. Palju tuleb ette tekste ja pöördumisi, mis sisaldavad isikuandmeid, aga on võõrkeeles. Tööd lihtsustaksid automaatsed tõlkevahendid, mis peavad olema aga sobivate andmekaitsetingimustega.

4.6 Majandus- ja Kommunikatsiooniministeerium

Majandus- ja kommunikatsiooniministeeriumi intervjuul rõhutati, et andmekaitse ja privaatsuseesmärkide saavutamine on tugevas seoses riigi küberturbepoliitikaga ning need saaksid areneda sünergias.

4.7 Politsei- ja Piirivalveamet

PPA näeb potentsiaali andmete taaskasutuses ning väliste arendajate kaasamises. Selleks on vaja leida turvalised ning õiguskindlad viisid andmete teisendamiseks anonüümsele kujule.

4.8 Päästeamet

Päästeamet töötleb tundliku iseloomuga andmeid ja soovib andmetele tuginedes edendada ennetustööd. Päästeamet soovib edaspidi infosüsteemide arenduses, teadustöös ja päästetöö juhtide väljaõppes kasutada sünteetilisi andmeid. Pikas perspektiivis oleks Päästeameti tööle suurima positiivse mõjuga statistika tegemise ja andmete jagamisega seotud lahendused, mis toetaksid teadlike otsuste tegemist, näiteks päästestrateegia uuendamist. Konkreetsemalt on Päästeametil vaja ka tööriista, mis puhastaks vabateksti isikustatavast osast, mis analüüsi jaoks oluline ei ole.

Päästeamet sooviks enda töös taaskasutada inimeste positsioneerimise ja liikuvusandmeid. Neid on vaja ennekõige operatiivsituatsioonides kasutamiseks, mille puhul mingis kohas just momendil toimub mingi sündmus, millega tegelemiseks on vaja täpselt teada, kui palju seal on inimesi ning tegelikult kõike muud, mida nende kohta on võimalik teada saada. Päästeametil ei ole seda infot vaja indiviidi tasemel vaid koondtulemitena.

Perspektiivis huvitab Päästeametit ka isikustatavate andmete vähendamine koostöös vabatahtlikega. Näiteks on töötajate ja vabatahtlike kohta Päästeametil vaja teada vaid asjaolu, kas isik on oma tööde täitmiseks piisavalt terve ning tervet haiguslugu ei ole vaja. Seejärel on vaja teada vaid muudatustest tervises, kui need välistavad ülesannete täitmise.

4.9 Rahandusministeerium

Rahandusministeeriumi erinevates vastutusvaldkondades on suur vajadus erinevate põhimääruste ja õigustega andmebaaside ühildamiseks ajakohase ja suure rakendusväärtusega analüütika tegemiseks. Poliitikavalikute sotsiaalmajandusliku mõju mudelite genereerimist parendaks isikustatud andmete kasutamise lihtsustamine. Üheks kõrge lisaväärtusega näiteks on asukoha- ja liikumisandmete kasutamine rände modelleerimisel, eriplaneeringute tegemisel.

Krediidipoliitikas on kaalumisel positiivse krediidiregistri kontseptsioon. Selle arendusel on kaalumisel olnud nii krediidisaajate (isikute) privaatsuse kui -andjate ärisaladuse kaitse. Süsteemi kasulikuks kõrvalefektiks oleks nii parem järelevalve vastutustundliku laenamise põhimõtete üle, kui parem läbipaistvus inimestele endile. Iga krediidivõtja saaks ühest allikast ülevaate kõigi enda kohustuste kohta.

Sotsiaalkindlustusametist, pensioniregistrist, pensionifondidest ning rahvastikuregistrist pärinevaid andmeid ühendades saaks luua kolme samba ülese pensioniportaali, mis pakuks väärtust nii inimese jaoks personaalselt kui ka avalikkusele.

Andmete kasutamiseks poliitikaanalüüsis on vaja korduvkasutatavaid lahendusi, mis saaks automaatselt uusi andmeid ja toetaks fiskaalpoliitikat pidevalt.

4.10 Rahvastikuregister

Sünteetiliste andmetega rahvastikuregistri kaksik toetaks teadustööd ja infosüsteemide testimist.

4.11 Riigi Infosüsteemi Amet

RIA arendab Bürokratti — Eesti riiklikku virtuaalset abilist. Teenuste kasutamise kratiliides vajab treenimiseks liitõpet, millega kaasneb oht kasutatavate andmete privaatsusele. Turvalisem oleks treenida sünteetilistel andmetel, mitte pärisandmetel.

Bürokrati sõnumivahetus toimub otspunktkrüpteeringuga. Ent kuna kodanik võib Bürokrati vahendusel sama seansi raames soovida suhelda mitme asutusega, vajab rakendus anonüümset klassifitseerijat, mis inimeselt saadud infost vaid vajalikke klassifikaatoreid tuvastades ja isikuandmeid kõrvaldades seansi ühest asutusest teise suunaks nii, et eelnevale asutusele ei jääks infot, kuhu ning mis põhjusel inimene edasi läks.

RIA kui vahendusteenuse pakkuja (autentimise, allkirjastamise, pääsuhalduse, seansihalduse jms kontekstis) peab nende toimingute käigus tekkivaid andmeid mh logima teenuse tööshoidmiseks, häiringute ja võimalike turbeintsidentide tuvastamiseks. Samamoodi tekivad rikkalikud logiandmestikud sündmusteenuste ja nõusolekuteenuse puhul. Teenuste pakkumiseks tagab RIA vajaliku info ühildamise, mis on seotud erinevate X-tee päringutega. Selliste teenuste edasisel lisandumisel on otstarbekas otsida võimalusi isikuandmete töötlemise minimeerimiseks privaatsuskaitse tehnoloogiatega.

4.12 Siseministeeriumi infotehnoloogia- ja arenduskeskus

SMIT näeb samuti potentsiaali ühiskonda toetavate analüüside ja statistika tegemisel, kus on olulised arvud, aga mitte see, millised isikud nende taga on. Anonüümimise tehnikaid kasutatakse testandmete loomiseks.

Keerukust loob pilvteenuste populaarsuse tõus. Pilveandmetöötluse omadused on skaleeruvuselt ja töökindluselt atraktiivsed, kuid isikustatud ja muidu tundlike andmete töötlemiseks mitte täielikult sobilik.

4.13 Sotsiaalministeerium

Sotsiaalministeeriumi haldusalas on näiteks tervishoiusüsteemi, terviseandmed ja sotsiaaltoetuste andmed, mis on poliitikaanalüüsis väga väärtuslikud. Nende tänase kasutuse keerukus on ennekõike seotud uuringu ettevalmistamise keerukuse ning loa menetlusprotsessi pika kestusega. Võib juhtuda, et mõni uuringuküsimus aegub või muutub.

Kõrge väärtusega oleks süsteem, kus erinevatest andmeallikatest pärit andmeid saaks sobivate tehniliste lahendustega siduda ja need oleksid kõikide andmeallikate omanikele õiguslikult vastuvõetavad ja kiiremini menetletavad. Lahendusena ei oleks vaja pidevalt eksisteerivat andmebaasi, mis ühendab kõik teised, vaid kiiret võimalust tellida registrite ülest andmete ühendamist konkreetsete tunnustega. Nii tekkiv andmestik võiks olla ka fikseeritud elueaga.

Praegu puudub ühtne ümarlaud, kus andmeomanikud saaksid andmetöötlusega seonduvatel teemadel arutleda ja vajadusel kokku leppida teatud asjade ühistelt ärategemises.

4.14 Statistikaamet

Riikliku statistika rahvusvaheline trend on uute andmeallikate kasutuselevõtt. Kõrget väärtust nähakse erasektori andmetes, mida täna kontrollivad sideettevõtted, finantsasutused, energeetikaasutused jt. Selliste andmete töötlemine riiklikus statistikas ei ole reguleeritud.

Privaatsuskaitse tehnoloogiad võiksid olukorda lahendada nii, et detailandmed ei liiguks eraettevõttest Statistikaametisse, kuid Statistikaamet saaks tulemuse ja võimaluse vajadusel kontrollida metoodikat. Andmete ühendamise vajadus teeb olukorra keerukamaks, sest lisaväärtust oodatakse just erasektori andmebaaside ühendamisest Statistikaameti andmebaasidega.

Vaja oleks tehnoloogiat, mis aitaks andmete töötlemisel (ennekõike ühendamisel ja rikastamisel) vähendada käsitööd ja sellest tulenevaid turvariske ning selgitada ühiskonnale, et selline linkimine toimub turvaliselt. Kui privaatsuskaitse tehnoloogiad aitaks luua ühiskondlikku tuge andmehõivele statistika otstarbeks, oleks see kindlasti tugev motivatsioon tehnoloogia kasutamiseks.

Statistikaamet soovib ka efektiivsemalt tööle saada riigi andmeringluse, ehk andmete jagamise riigiasutuselt teisele riigiasutusele. Statistikaamet ei või anda statistika jaoks kogutud isikustatud andmeid teisele asutusele isegi siis, kui viimasel on nende andmete valdamiseks õiguslik alus. Andmehaldusteenuse osas on soov taset tõsta ja riigi käsutuses olevate andmete pealt avalikule sektorile veelgi rohkem lisandväärtust luua, seejuures inimeste privaatsust säilitades.

4.15 Tervise- ja Heaolu Infosüsteemide Keskus

TEHIK arendab süsteemseid ja korduvkasutatavaid andmeanalüüsi lahendusi, mis juba rakendavad ka privaatsuskaitse tehnoloogiaid. Tulevikus on peamine ülesanne uute liideste loomisel Euroopa tervisevaldkonna andmeruumidega, erasektori tervishoiuteenustega, digitaalse tervise rakenduste ja otsusetoe süsteemidega. Kõik sellised lahendused võivad vajad erinevaid tehnilisi ja õiguslikke lahendusi.

Tehnilistest vajadustest tõsteti esile nii struktureeritud andmete kui vabateksti pseudonüümimist ja anonüümimist. TEHIKul on eelnimetatud valdkondades kogemusi, kuid pseudonüümimise ja anonüümimise tehnikate puhul on vajadus pidevalt kursis olla sellega, milliseid ründevektoreid nõrgalt anonüümitud andmete taasisikustamiseks olemas on.

TEHIK on loonud sünteetilisi testandmeid, kuid soovib neid teha nii, et need oleksid pärisandmetele sarnasemad, aga samas isikutega mitteseostatavad. Vaja oleks üldist lähenemist testimisel ja arendusel vajalike andmete tootmiseks.

4.16 Tervisekassa

Tervisekassa on arendamas andmete analüüsiks ajaloolise vaatega andmeladu. Kvaliteetsete analüüside jaoks on vaja kasutada erinevatest allikatest pärit isikustatud andmeid, et koostada näiteks terviseteekondi ja analüüsida ravi tulemuslikkust. Sotsiaalvaldkonnas saaks andmete toel kirjeldada sihtgruppe (nt inimesed, kes elavad üksi või vajavad mõnda konkreetset toetusmeedet või teenust). Seejärel saaks mõõta nende gruppide suurust ning hinnata toetuse või teenuse investeeringuvajadust.

Andmete ühendamise protsess peaks olema efektiivsem, et andmete kokkupaneku ja analüüsi tulemusteni jõutaks kiiremini. Kasu oleks standardteenustest ja sisse töötatud rollijaotuses.

4.17 Transpordiamet

Transpordiameti peamine huvi on mitmest allikast andmete analüüs ennetuse eesmärgil. Andmeid on vaja vaadata nii isiku kui sõiduki tasemel (ajalugu, ülevaatused jne). Selleks sobivat lahendust on Transpordiamet otsimas. Samuti näeb Transpordiamet, et keskne teadmuse haldus ja koolitusvõimalus aitaks üleriigiliselt tööd lihtsustada.

5 Poliitikasoovitused

5.1 Teadlikkuse tõstmine privaatsusest ja privaatsuskaitse tehnoloogiatest

5.1.1 Elanikkonna teadlikkuse tõstmine privaatsusest

Kollektiivne turvalisus algab indiviidi teadlikkusest ja oskustest oma privaatsust kaitsta või nõuda selle kaitsmist teistelt osapooltelt. Leitud on, et digiühiskonnas, kus algoritmid suunavad üha rohkem üksikisikute käitumist ja harjumusi, on privaatsusest saanud erakordne hüve, mille tagamiseks on vaja teha teadlikke samme[45]. Privaatsuse teadvustamine ühiskonnas on praeguses digimaailmas väga oluline. Inimesed ise peavad võtma teadliku rolli oma väärtuslike andmete kaitsmisel ja käituma nendega heaperemehelikult. Privaatsuse sisu võib sõltuda konkreetsest isikust ja olukorrast. Seda teadvustab ka andmekaitseõigus, mis kehtestab eriliigiliste andmete töötlemisele kõrgemad nõuded. Ühelt poolt peab üksikisik olema ise piisavalt teadlik oma õigustest ja käituma enese andmetega vastutustundlikult, teisest küljest peab ka nende andmete töötleja tegema kõik endast sõltuva, et andmesubjekti õiguste rakendamine oleks võimalikult lihtne. Eriti oluline on see juhul, kui andmesubjektiks on laps. Intervjuudes toodi välja ka inimese enda tahet ja selle avaldamise võimalust suhtes e-riigi teenustega. Inimesel endal peaks jääma viimane sõna selle osas, kas ta soovib mingit teenust või hüvitist, näiteks soodustavate proaktiivsete teenuste osas.

Soovitused:

1. Privaatsuse teadvustamine ühiskonnas on väga oluline. Ühe võimalusena saab teha erinevaid kampaaniaid vastavalt sellele, kus sihtrühm seda kõige tõenäolisemalt tarbib. Privaatsusteemade põimimine näiteks kooliõppe digioskuste kavasse annaks kindlasti pikemas plaanis efekti.
2. Selleks, et teadmine privaatsuskaitse tehnoloogiatest, sealhulgas täna vähem tuntud läbipaistvuse ja sekkutavuse tehnoloogiatest jõuaks suure hulga inimesteni, oleks vajalik asjaomase info levitamist keskselt organiseerida, määrata vastutaja ja mõõdikud, mille alusel oleks võimalik hinnata, kuidas on ajas muutunud tehnoloogia- ja õiguskogukondade teadlikkus PET-idest. Lisaks sellele, et teadlikkus tõuseb, tuleks praktilise soovitusena esitada ka näiteid, kuidas saab indiviid teha teenuste vahel valikuid selle järgi, kuidas need tema andmeid kaitsevad. Kaardistada tuleks algtase ja olukord teatud aja pärast, mis võimaldaks hinnata, kas PET-ide kasutamine teenustes on muutunud ajas populaarsemaks või milliste PETide kasutus on osutunud praktikas hõlpsamaks.
3. Üks võimalus oleks teadlikkuse tõstmine PET-idest ka läbi haridussüsteemi ja koolituste. Ülikooli tasemel katavad valdkonda õppeained arvutiteaduse valdkonnas, kuid süsteemsem lähenemine, mis kataks näiteks ka juriidilist õpet ja IT-õigust, täna puudub.
4. Läbi tuleks mõelda ka meetmete jätkusuutlik rahastamine.

Intervjuudes toodi välja ka ühiskonna harimise vajadust. Ühiskonna toetus ja vastuvõtt (ingl k *social licensing*) andmehõivele ja -kasutamisele tuleb saavutada enne, kui andmehõivet ennast teostama hakatakse. Rahvusvahelises kogemuses on esinenud olukordasid, kus organisatsioonil on küll õigus teatud andmete töötlemiseks, kuid ühiskonna madal teadlikkus ja kaheldava

[45] ERR, Andra Siibak: laste privaatsusõigus andmerikkas maailmas, https://dspace.ut.ee/handle/10062/66433 (Viimati külastatud 27.02.2023).

väärtusega meediakajastus on tekitanud ühiskondliku vastuseisu. Privaatsuskaitse tehnoloogiate mõistliku rakendamise ning läbipaistvuse ja sekkutavuse lahenduste loomise abil saaks ühiskondlikku toetust hõlpsamini suurendada ning leevendada inimeste hirme oma andmete riigi ja eraettevõtetega jagamise ees.

Soovitused:

1. Rakendada andmejälgija kõikidesse e-riigi teenustesse.
2. Tutvustada nõusolekuteenust ja selle võimalusi.

5.1.2 Teadlikkuse tõstmine privaatsuskaitse tehnoloogiatest avalikus sektoris

Intervjuude analüüsist selgub, et avalikus sektoris on privaatsuskaitse tehnoloogiatest teadlikkus olemas ja neid ka rakendatakse (näiteks pseudonüümimist, anonüümimist, piirangutega liideseid, analüütiku töökohtasid) või katsetatakse (diferentsiaalprivaatsust, liitõpet, sünteetilisi andmeid, usaldatavaid täitmiskeskkondasid, homomorfset krüptograafiat). Samas varieerus teadlikkus organisatsioonide lõikes, sõltudes teatud juhtudel ka asjaolust, millise valdkonna spetsialistiga intervjuu läbi viidi. Teadlikkus teatud tehnoloogiatest nagu näiteks pseudonüümimine ja anonüümimine on kõrgem kui teiste privaatsuskaitse tehnoloogiate osas. See võib olla tingitud asjaolust, et pseudonüümimist ja anonüümimist üldise (ja vastavatest tehnoloogiatega mitte perfektselt seotud tähendusega)) on nimetatud näiteks IKÜMis, millega on kursis suur osa avaliku sektori ametnikke. Samuti on need mõnevõrra lihtsamad ja inimeste jaoks arusaadavamad tehnoloogiad. Ka andmesünteesi puudutati paljudes intervjuudes. Vähem teati side ja identiteedi kaitsega seotud tehnoloogiaid ning läbipaistvuse ja sekkutavuse lahendusi, mis on keerukamad või pole laialdaselt kõlapinda saanud. Intervjuudest kõlas ka, et andmekaitsealane teadlikkus erinevates organisatsioonides on erineval tasemel ja selle ühtlustamisega tuleb tegeleda.

Oleme üha teadlikumad digitaalse teabega seotud riskidest ning selle mõjust isikuandmete töötlemisele, samas teadmised privaatsuskaitse tehnoloogiatest ning nende rakendamisest on alles lapsekingades. Samuti on era- ja avalikus sektoris veel vähe praktikat süsteemide talitluse kavandamisel nii, et töödeldavate andmete hulk oleks võimalikult väike ning kataks vaid eesmärgi saavutamiseks vajaliku.

Soovitused:

1. Selleks, et organisatsioon saaks privaatsuskaitse tehnoloogiaid rakendada, on vaja teadlikkuse tõstmist. Vahel eeldab piisava privaatsuskaitse taseme saavutamine ka erinevate tehnoloogiate kombineerimist – näiteks analüütiku töölaud, kus on vaid anonüümitud andmed. Selleks on vaja aga teadlikkust erinevatest privaatsuskaitse võimalustest. Selleks on sobilikud näiteks asjaomased koolitused, mis võimalusel arvestaksid konkreetse organisatsiooni eripärade ja vajadustega ning tooksid näidisrakendusi, millega on kergem suhestuda.
2. Teadlikkuse tõstmine võimaldaks avaliku sektori asutustel olla teadlikumad hankijad. Juba hanget ettevalmistavas faasis oleks võimalik mõelda sobilike privaatsuskaitse tehnoloogiate valikule ning privaatsustehnika rakendamisele. Vastavad tingimused tuleb hanke tingimustesse korrektselt lisada. Selleks sobivad samuti koolitused, aga ka konsultatsioonid valdkonna spetsialistidega.
3. Privaatsustehnika elementide ja privaatsuskaitse tehnoloogiate tuleks lisada digiriigi ristfunktsionaalsete nõuete sekka ja asutuste mittefunktsionaalsete nõuete dokumentidesse. Täpsemad nõuded tuleb välja selgitada eraldi analüüsi käigus.

4. Vastutustundliku andmekasutuse põhimõtete juurutamine avalikus sektoris[46].

5.2 Privaatsuskaitse tehnoloogiate valik ja rakendusesse sobivuse hindamine

5.2.1 Privaatsuskaitse tehnoloogiate võrdlemise ja riskianalüüsi meetodid

Privaatsuskaitse tehnoloogiate kaalumise ja kasutuselevõtu otsused on eeskätt seotud teadlikkuse tõusuga. Kui see on saavutatud, on järgmine samm sobiva tehnoloogia valik. Esmalt on tarvilik andmetele asjakohase kaitsetarbe määramine, et teada saada, millistel andmetel kui tugevaid kaitsemeetmeid oleks mõistlik kasutada. See omakorda eeldab ka tehniliste kaitsemeetmete hindamist, et oleks võimalik analüüsida, millised on parimad kaitselahendused lähtuvalt konkreetsetest andmetest ja nende kaitsetarbest. Selleks on vaja asjakohaseid riskianalüüsi meetodeid, mis aitaksid mõista erinevate PET-ide kasutamise riske ja eeliseid. Teatud meetodeid on juba olemas, näiteks saab leida tehnoloogia ja rakenduse jaoks lühima sammude hulga, millega keegi saab pseudonüümitud või anonüümitud andmetest isiku tuvastada. Kui see sammude arv tundub jõukohane isikule, keda hindaja ette kujutab, tuleks valida tugevam tehnoloogia.

Soovitused:

1. Sobivate privaatsuskaitse tehnoloogiate riskianalüüsi meetodite väljatöötamiseks oleks vaja analüüsida vastavat kirjandust ja koos õigusspetsialistidega hinnata, millisest keerukuse tasemest alates saab lugeda taasidentifitseerimise pingutuse ebamõistlikuks IKÜMi pp 26 mõttes. Tuleb arvestada, et mõned ründed muutuvad ajas lihtsamaks ja odavamaks või on lihtsamad kellelegi, kellel on juurdepääs täiendavatele andmetele või võimalik need saada. Selliseid riskianalüüse saab teostada teenusepakkuja asutuses või tellida teadlastelt või erasektorist, näiteks privaatsusmõju analüüsi osana. Vaja on tagada ka selliste uuringute või analüüside teostamise rahastus.
2. Andmekaitse ja infoturve peaksid olema standardne osa mittefunktsionaalsetest nõuetest.

Privaatsuskaitse tehnoloogiate kontekstis on oluline tehnoloogianeutraalsuse printsiibi järgimine, seda eeskätt õigusloomes. See on vajalik, et tehnoloogiliste arenduste tegemine ei oleks pärsitud ning nõuded ei kirjutaks ette konkreetset toodet või platvormi vaid sellega saavutatavaid omadusi.

Soovitused:

1. Uute normide kehtestamisel või olemasolevate muutmisel tuleb järgida, et lähtutakse tehnoloogianeutraalsuse printsiibist. Näiteks, kui soovitakse, et teatud andmetöötlusprotsesside puhul rakendatakse täiendavaid kaitsemeetmeid, siis tuleks jääda võimalusel üldisele tasemele, et andmetöötlejal oleks võimalus hinnata keskkonda, kus andmetöötlus toimub, ja sellega seotud riske, mille põhjal on võimalik kavandada asjaomaste kaitsemeetmete rakendamine. Näiteks võib nõuda, et volitatud töötleja jaoks peab olema andmete taasisikustamine seotud ebamõistliku pingutusega.

Tulevikukindla digiriigi ehitamine ja kaasaegsete, inimkesksete e-teenuste loomine on pidev protsess.

[46] Justiitsministeeriumi eestvedamisel erinevaid osapooli koondanud ekspertrühma poolt 2020. aasta alguseks välja töötatud "Isikuandmete vastutustundliku töötlemise põhimõtted" https://www.just.ee/media/3134/download (Viimati külastatud 03.03.2023).

Soovitused:

1. Vajalik on oluliste privaatsuskaitse tehnoloogiate ning läbipaistvuse ja sekkutavuse tehnoloogiate analüüs ja valimine.
2. Andmepõhise otsustamise lahenduse jaoks tuleks teostada sobivate privaatsuskaitse tehnoloogiate kaardistus.
3. Sündmusteenuste jaoks tuleks luua turvalised andmeruumid.
4. Kasutusse tuleb võtta privaatsust säilitav autentimise logimine ja anomaaliate tuvastamine.
5. Tuleviku e-ID tuleb siduda privaatsuskaitse tehnoloogiatega. Selleks tuleks uuendada vastava sisuga eID valget raamatut.

5.3 Privaatsuskaitse tehnoloogiate rakendamiseks vajalik ressurss

5.3.1 Rahaline ja inimressurss

Intervjuudest selgus, et privaatsuskaitse tehnoloogiate rakendamist tajutakse kulukana (kuigi sellega seotud hinna kasvu keegi välja ei toonud). Küll aga tajutakse vajadust tööprotsesside ümber korraldamiseks. Nenditi, et selleks ei ole praegu ei rahalist ega tööjõu ressurssi. Ilma lisarahastuseta ei peeta tehnoloogiate rakendamist võimalikuks.

Soovitused:

1. Organisatsioonides tuleks esiteks selgeks teha, milliseid andmete analüüsiga ja süsteemide testimisega seotud tööprotsesse on võimalik automatiseerida, et tekitada olemasolevale personalile aega sisukamate ja olulisemate küsimuste ja teemadega tegelemiseks. Suuremat efektiivsust loovad automatiseeritud protsesside ideed tuleks kavandada eelarvesse, vajadusel taotleda lisarahastust. Tööprotsesside efektiivsemaks muutmine sõltub ka selles kasutatavast tarkvarast.
2. Näha ette lisarahastus avaliku sektori andmeanalüütika tööprotsesside ülevaatamiseks ja lihtsamate tööde automatiseerimiseks.

5.3.2 Protsesside automatiseerimine

Intervjuudest selgus, et enamik organisatsioone kasutab teatud privaatsuskaitse tehnoloogiaid, kuid nendega on seotud palju käsitööd. Näiteks isikuandmete pseudonüümimisel või anonüümimisel võiks töö mingis mahus usaldada tehnoloogiale, mis võimaldaks hoida kokku väärtuslikku tööaega ja ametnikul oleks võimalik keskenduda keerukamate ülesannete teostamisele. Protsesside automatiseerimisega on võimalik saavutada inim- ja rahaliste ressursside kokkuhoid.

Soovitused:

1. Tuvastada rutiinsed ja korduvad protsessid või töövood, mis on seotud privaatsuskaitse tehnoloogiatega ning need automatiseerida. Läbi tuleks mõelda võimalikud rakendatavad tehnoloogiad, et pakkuda kaitset sellistele protsessi või töövoo osadele või nendes töödeldavatele andmetele, mis vajavad tõhusamat kaitset.

5.4 Andmetega seotud soovitused

5.4.1 Sünteetilised andmed ja digitaalsed kaksikud kui teenuste ja protsesside turvalise arendamise ja testimise võimaldajad

Intervjuudest selgus, et mitmetele asutustele oleksid suureks abiks sünteetilised andmed või nn digitaalsed kaksikud, kus teenuste arendamiseks, protsesside loomiseks või nende testimiseks oleks võimalik kasutada sünteetilisi andmeid või digitaalseid kaksikuid, mis asendaksid reaalelu andmeid, olles oma struktuurilt, omadustelt ja seostelt väga sarnased päris andmetega. Selleks, et saada päriselulistele andmetele omadustelt sarnaseid andmeid, saab kasutada sünteetiliste andmete genereerimist analüütiliselt koostatud mudeleid kasutades.

Soovitus:

1. Riigil tuleks kaardistada valdkonnad, kus sünteetiliste andmete või digitaalsete kaksikute kasutamine teenuste arendamiseks, protsesside loomiseks või nende testimiseks annaks suurima efekti. Seejärel tuleks teostada pilootprojektid ja välja ehitada jagatud testkeskkond ja teenused.

5.4.2 Andmete ühekordse küsimise põhimõte

Andmekogusse andmete kogumisel lähtutakse andmete ühekordse küsimise põhimõttest (AvTS § 43^1 lõige 3). Andmete ühekordse küsimise põhimõtte rakendamine vähendab andmete esitajate halduskoormust aga tagab ka riigi tõhusama toimimise. Kui organisatsioonil on temale seadusega või seaduse alusel antud ülesannete täitmiseks vaja töödelda andmeid, mis on juba ühes andmekogus olemas, siis ei tohiks neid enam täiendavalt küsida ja olemasolevaid andmeid tuleks n-ö taaskasutada. Teadaolevalt ei ole see põhimõte veel täies ulatuses rakendunud, arvestades teatud andmete puhul kehtestatud piiranguid.

Soovitus:

1. Kaardistada tuleks, millised organisatsioonid küsivad (teadlikult, teadmatult või vastava regulatiivse nõude tõttu) andmete esitajalt infot, mis tegelikult riigi mõne teise organisatsiooni käes juba olemas on. Seejärel oleks vaja analüüsida, kas vastavad protsesse oleks võimalik viia kooskõlla andmete ühekordse küsimise põhimõttega.

5.4.3 Andmete kvaliteet

Intervjuudes tõsteti pidevalt esile ka andmete kvaliteediga seotud probleemkohtasid. Keeruline on teha erinevat analüütikat, kui andmete kvaliteet on madal, samamoodi võivad kannatada ka tulemused ja nende pinnalt tehtavad otsused. Seevastu hea kvaliteediga ja usaldusväärsed andmed võimaldavad saavutada lisaväärtust.

Soovitus:

1. Organisatsioonides tuleb leida andmestikud, mille kvaliteedi tõstmisel oleks kõige tugevam efekt. Tuvastada on vaja organisatsiooni eripäradest tulenevalt kõige sobilikumad vigaste andmete parandamise meetodid. Samuti tuleks tegeleda ka ennetava poolega, näiteks analüüsida, kuidas on võimalik vigaste andmete tekkimist ennetada, selleks vastavaid infosüsteeme või protsesse muutes.

5.4.4 Avaandmed

Avaliku sektori loodud või kogutud andmed peaksid ühiskonnale kasu tooma. Direktiiviga (EL) 2019/1024 ja liidu valdkondliku õigusega tagatakse, et avaliku sektori asutused teevad rohkem enda loodavaid andmeid kasutamise ja taaskasutamise eesmärgil kergesti kättesaadavaks (andmehalduse määrus, pp 6). AvTS § 3^1 lõike 3 kohaselt peab teabe üldiseks kasutamiseks andmisel olema tagatud isiku eraelu puutumatus, autoriõiguste kaitse, riigi julgeoleku kaitse, ärisaladuse ja muu juurdepääsupiiranguga teabe kaitse.

Enne teabe üldiseks kasutamiseks andmist peab teabevaldaja hindama teabe üldisele kasutamisele piirangute kehtestamise vajadust. Kui seaduse alusel avalikustatav teave sisaldab isikuandmeid, võib selle üldist kasutamist piirata, kui see kahjustab oluliselt isiku eraelu puutumatust (AvTS § 3^1 lõige 7). Kui seaduse alusel avalikustatava ja isikuandmeid sisaldava teabe üldiseks kasutamiseks andmine kahjustab isiku eraelu puutumatust, antakse see üldiseks kasutamiseks viisil, mis ei kahjusta oluliselt isiku eraelu puutumatust (AvTS § 3^1 lõige 8). Intervjuudest selgus, et praegusel juhul on avaandmete avalikustamine keeruline, kuna on suures osas käsitöö ja kokkulepete küsimus. Samas on avaandmetega seoses tuntud muret, et ilma tugevate andmekaitsemeetmeteta võib tekkida risk, et digimajandus ei ole kestlik. Kuigi andmete taaskasutamine, jagamine ja kättesaadavus on kasulik, võib see põhjustada ka kahju andmesubjektidele ja ühiskonnale tervikuna[47]. Seetõttu on hästi oluline tegeleda privaatsuskaitse tehnoloogiatega, neid arendada, analüüsida, hinnata, katsetada ja rakendada, et isikud julgeksid oma andmed usaldada turvaliselt riigi kätte.

Soovitused:

1. Andmete mitteisikustavale kujule teisendamiseks on mitmeid sobivaid privaatsuskaitse tehnoloogiaid, nagu diferentsiaalprivatsus ja sünteetiliste andmete genereerimine.
2. Andmebaasi anonüümsele kujule teisendamine on töötlemine ja vajab õiguslikku alust ning kooskõla töötlemise eesmärkidega. Oluline on, et testimiseks või avaandmeteks võib avaldada vaid privaatsuskaitse tehnoloogiaga töötlemise tulemina saadud andmeid.

5.4.4.1 Andmete töötlemine pilvandmetöötlusega

Avaliku sektori võimekus kasutada pilvandmetöötluse lahendusi on suuresti piiratud andmekaitse ja küberturvalisuse nõuetega. Pilvteenustega seotud murekohti jagati ka intervjuude käigus. Näiteks nenditi, et tulevik ja tootjad suunavad teenused ja andmed pilvandmetöötlust kasutama. Organisatsioonidel on teatud pilvteenuste vastu suur huvi, kitsaskohtadena toodi välja ka seadusandlust või seda, et üksikul organisatsioonil ei ole võimalik suurte pilvteenuseosutajatega tingimusi läbi rääkida. Toodi välja, et mõned riigid keskselt koordineerivad lepingutingimusi suurte pilvteenuste osutajatega, mis laienevad seejärel terve riigi avaliku sektori organisatsioonidele, kes viidatud ettevõtte teenused kasutusse võtavad.

Soovitused:

1. Anda organisatsioonidele suunised, milliseid andmekaitselisi ja küberturbega seonduvaid nõudeid tuleb järgida pilvteenuste valikul.
2. Kaardistada, milliste pilvteenuseosutajate teenuste vastu enim riigis huvi tuntakse, ja mõelda keskselt lepingutingimuste läbirääkimise peale.

[47] Euroopa Andmekaitsenõukogu, Avaldus 05/2021 andmehaldust käsitleva õigusakti kohta seoses õigusloome suundumustega Vastu võetud 19. mail 2021. - Internetis kättesaadav: https://edpb.europa.eu/system/files/2021-08/edpb_statementondga_19052021_et.pdf (Viimati külastatud 02.03.2023).

3. Analüüsida tuleks erinevate privaatsuskaitse tehnoloogiate kasutamise võimalusi eriliigiliste isikuandmete töötlemisel mitte-Euroopa andmekeskustes ja pilves, mis tagaks IKÜMi kohase kaitse.

Teatud juhtudel on võimalik avalikul sektoril kasutada üksnes Eesti riigipilve. Sellelt oodatakse majanduslikku efektiivsust.

Soovitused:

1. Analüüsida riigipilvega seotud kulude efektiivsust.

5.4.5 Suurandmetöötlusega seotud õiguskeskkond

Mitme intervjuu käigus toodi välja, et suurandmete töötlemiseks puudub käesoleval ajal piisav õigusselgus. Sooviti, et seadusandlus toetaks rohkem innovatsiooni. Viidati ka AvTSile kui paberiaja seadusele. Mitmed organisatsioonid sooviksid teha valitsemisalaga seotud otsuseid, mis tugineksid kvalitiivsetel andmetel. Soovitakse, et avalik sektor ja poliitika kujundajad võtaksid otsuste tegemisel, mida tuleb teha üha kiiremini, arvesse maailmas toimuvaid muutuseid, kaasates samas järjest suuremat hulka erinevas formaadis andmeid [48]. See aga on keerukas, kuivõrd praegune õiguskeskkond ei ole selleks piisav. Õiguskirjanduses on välja toodud suurandmetöötluseks sobiva õigusliku aluse puudumist. Tegemist on valdkondadeülese probleemiga, mis vajab süsteemset lähenemist. Samas tuleb koheselt mõelda ka andmesubjektide õiguste ja vabaduste tagamise küsimustele ning asjaomaste privaatsuskaitse tehnoloogiate, aga ka läbipaistvuse ja sekkutavuse tehnoloogiate võimalikule rakendamisele, mis lisaks kaitse funktsioonile pakuks andmesubjektile ka kindlustunnet, et tema privaatsus on võimalikult parimal moel kaitstud ning ta saab seda mõjutada. Seeläbi säiliks ja kasvaks usaldus riigi ja riigis toimuva andmetöötluse vastu.

Soovitused:

1. Kaardistada õiguskeskkonna ebapiisavused, mis takistavad poliitikakujundamiseks vajalikku suurandmetöötluse läbiviimist. Kõige suurema murekohana on nähtud suurandmetöötluseks sobilike õiguslike aluste puudumine. Iga ministeerium võiks üle vaadata oma valitsemisala vastavad vajadused ja seejärel oleks vaja keskset koordineerimist, kuidas asjaomaste seaduslike ettepanekutega edasi liikuda. Ühe mõttena on toodud, et kui iga organisatsiooni puhul kehtestatakse massandmetöötluseks erimeetmed eriseadustes, vähendab selline olukord õigusselgust, mitte ei lahenda probleemi. Seetõttu vajaks eraldi diskussiooni, kas suurandmetöötluseks oleks vajalik kehtestada üldine, valdkondadeülene regulatsioon, mis sätestaks põhimõtted, millest suurandmetöötlusel lähtuda tuleks. Igal juhul on soovitatav asjaomastes seaduslikes ettepanekutes hõlmata ka tingimused, milliseid kaitsemeetmeid peaks asjakohase õigusliku aluse kasutaja üksikisiku privaatsuse võimalikult väheseks riivamiseks ja tema isikuandmete kaitsmiseks rakendama.
2. Lisaks sobivate õiguslike aluste loomiseks ja seega kindlustunde pakkumiseks organisatsioonidele on vaja kindlustunnet säilitada ka üksikisikutes. Seetõttu tuleks suurandmetöötlus siduda tõhusate kaitsemeetmete rakendamisega. Ühe lahendusena on võimalik kasutada privaatsuskaitse tehnoloogiaid ning läbipaistvuse ja sekkutavuse lahendusi selliselt, et organisatsiooni poolt soovitud andmetöötluse puhul ei näe organisatsioon konkreetseid algandmeid, sh isikuandmeid (kui need andmed ei asu tema enda peetavas andmekogus),

[48] Riigikantselei, Andmepõhine otsustamine, https://www.riigikantselei.ee/valitsuse-too-planeerimine-ja-korraldamine/valitsuse-too-toetamine/andmepohine-otsustamine (Viimati külastatud 27.02.2023).

vaid saab soovitud tulemi üldistatud kujul, näiteks statistikana, mis võimaldaks teha andmepõhiseid otsuseid soovitud ajahetkel.

3. Abiks võiksid olla ka mitme andmekogu andmete privaatset sidumist võimaldavad tehnoloogiad. Ka siin saab ühiste lahenduste loomisega jõuda tulemuseni efektiivsema ressursikuluga.

5.4.6 Suurandmetöötlusega seotud protsessid

Suurandmete töötlemise protsess on keerukas, loakohustus suurandmetöötlusel tekitab segadust, näiteks kellelt ja millal on vaja luba, et protsess on pikk, ja otsust on vaja kiiremini kui sisse töötatud protsess lubab. Sellise andmetöötluse jaoks vajatakse tihti kas Andmekaitse Inspektsiooni või mõne eetikakomitee luba, mille taotlemine võib võtta aega. Poliitikakujundamiseks ja vajalike otsuste tegemiseks peaks suurandmetöötlus toimuma vajaduspõhiselt ja võimalikult efektiivselt. Mitmed intervjueeritavad ütlesid, et kuivõrd puudub hea ülevaade protsessidest (konkreetsetest sammudest, mida tuleb astuda sellise andmetöötluse õiguspäraseks läbiviimiseks) ja õiguskindlus, siis jäetakse mõnikord soovitud andmetöötlus üldse tegemata ja toetutakse muudele, kiiremini kättesaadavatele allikatele, mis paraku ei pruugi anda nii kvaliteetset infot, kui seda saaks soovitud andmetöötlusest. Leiti ka, et näiteks teadustöö raames, mis hõlmavad mitme erineva vastutava töötleja andmekogusid, ei ole ühtset praktikat selle osas, milline vastutav töötleja peaks andmed kokku panema. Nenditi, et selliselt ei ole võimalik riigi poolt kogutud andmeid käesoleval ajal kiiresti poliitikate kujundamise tarbeks kasutada. Suurandmete töötluse probleemid ei ole üksnes regulatiivsed. Esineb ka tehnilisi takistusi, nt on välja toodud, et X-teel on käesoleval ajal ebamugavusi tervete andmebaaside vahetamisega[49], kuivõrd X-tee on loodud pigem väiksemahuliste päringute ja edastuste korral.

Soovitused:

1. Lihtsustatud ja visuaalne suunis loakohustuse protsessist koos valdkondlike näidetega aitaks suurandmetöötlusega seotud protsesse, mida ametnik peab läbima, paremini mõista. Samuti oleks abiks ka ühtsete põhimõteteni jõudmine erinevate osapoolte vahel ja asjaomaste suuniste avaldamine.
2. Ühe võimalusena oleks võimalik kaaluda riigi poolt keskse turvalise suurandmete vahetamise keskkonna loomist, mis annaks võimaluse ka privaatsuskaitse tehnoloogia keskseks rakendamiseks.

5.4.7 Üldised andmetega seotud protsessid

Andmetega seotud protsessid on vaja teha selgeks. Selleks, et organisatsioonid paremini mõistaksid, kuidas andmed riigis liiguvad, oleks hea joonistada üles riigisisesed protsessid, kuidas üldse andmete kasutamine käib erinevate (vajaduste), näiteks teadustöö tarbeks. Märkida tuleks, millistel juhtudel on vaja eetikakomitee või Andmekaitse Inspektsiooni luba. Iga üksik ärivaldkonna inimene ei pea teadma tehnoloogilistest võimalustest, vaid seda teadmust on vaja teatud protsessi osas ja seda võiks pakkuda kompetentsikeskus, kes seda teadmist omab.

Soovitused:

1. Abiks võiks olla andmekaitse liivakast või kompetentsikeskus, kus oleks võimalik andmekait-

[49] Andmekaitse Inspektsioon, Andmeladude seire kokkuvõte, Seire järelduse punkt 5. – Internetis kättesaadav: https://www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf (Viimati külastatud 02.03.2023).

sega seotud küsimusi arutada.

2. Iga andmekogu vastutav töötleja peaks seadma üles ühe kontaktpunkti, kes vastutab andmete väljastamise protsessi eest, suudab seda toetada ning saab öelda, milliste tehnoloogiatega on tema andmete töötlemine vastuvõetav.
3. Tehnoloogia tööriistakast, mille atribuutidega oleks protsessi teatud osades võimalik sekkuda. Pelgalt tööriistadest ei piisa, kaasa peaks tulema ka vastav kompetents, nt konsultatsioonidena.
4. Andmekaitse Inspektsioon võiks jagada parimaid praktikaid.

5.4.8 Andmehalduse korraldamine kriisi- või sõjaolukorras

Teadaolevalt ei ole praegusel hetkel paigas konkreetseid plaane, kuidas korraldada andmete logistikat kriisi- või sõjaolukorras või ühe olukorra eskaleerumisest teise.

Soovitus:

1. Tuleks analüüsida olukorda, kui teatud ajahetkedel ei ole võimalik käidelda andmeid ettenähtud viisil, nt andmekeskuste töö on häiritud või pole enam võimalik, milliseid on alternatiivsed tegevused viidatud olukordades, kas olemasolevaid kriisiplaane tuleks täiendada ja täpsustada ka andmetega seotud vaatenurgast, milliseid alternatiivseid kommunikatsiooniviise oleks võimalik kasutada turvaliseks infoedastuseks nii avaliku sektori sees kui ka suhtlemiseks elanikkonnaga.

5.4.9 Andmete puhastamise korraldamine

Andmete töötlemisel, eriti nende jagamisel kas organisatsiooni siseselt, kuigi rohkem väljaspoole organisatsiooni, tekivad erinevad küsimused andmete puhastamisega seonduvalt. Intervjuudest selgus, et andmete puhastamine on siiani suures osas käsitöö, kuigi erinevaid lahendusi on olemas ka andmete automaatseks puhastamiseks. Teema on samuti seotud avaandmete ja nende avalikustamisega.

Soovitused:

1. Andmete puhastamisel oleksid abiks analüütiku töökohad ning pool-automaatsed andmetest, tekstist või muust meediumist isikustatavate andmete eemaldamise tööriistad.
2. Intervjuudes leiti, et kasu oleks ka parimate praktikate vahetamisest organisatsioonide vahel, teadmiste jagamine erinevatest võimalustest ja tehnoloogiatest, mida saab kasutada efektiivseks andmepuhastuseks.

5.5 Muud kaardistatud teemad

5.5.1 Avaliku sektori töövoogude digiaega viimine

Läbiviidud intervjuudest kumas läbi avaliku sektori suur töömaht, töötajate puudus või olemasolevate töötajate ülekoormus. Tegemist ei ole otseselt andmete või andmekaitsega seotud teemaga, kuid teatud protsesside optimeerimise puhul, mis võimaldaks keskenduda olulisimale, saaks edukalt rakendada ka viidatud tehnoloogiaid.

Soovitused:

1. Töömahu vähendamine on võimalik läbi protsesside optimeerimise ja automatiseerimise. Mit-

med intervjueeritavad nägid võimalusi lihtsate ja rutiinsete ülesannete automatiseerimiseks, mis oleks võimalik usaldada tehnoloogiale. Nii oleks võimalik ametnikul keskenduda keerukamate ülesannete teostamisele ja raskemate küsimuste analüüsimisele. Selleks oleks vaja aga jagada teadmisi, parimaid praktikaid ja tööriistu. Selleks oleks vajalik esmalt kaardistada sellised avaliku sektori töövood ja protsessid, mida on võimalik automatiseerida.

2. Asjakohaste analüüsitööriistade rakendamine.
3. Tagatud peab olema ka eelnimetatud meetmete jätkusuutlik rahastamine.

5.5.2 Aktiivsem rahvusvaheline suhtlus ja innovaatiliste lahenduste osas tugevam sõnajõud Euroopas

Eesti on maailmas tuntud kui edukas e-riik. Intervjuudest kõlas, et veelgi enam eeldaks ametnikelt rahvusvahelist suhtlust ja innovaatiliste lahenduste osas ideede presenteerimist ja selles valdkonndas n-ö pildil olemist.

Soovitused:

1. Ametnike koolitused (esinemis-, veenmis- ja keeleoskuste arendamine).
2. Innovatsiooni propageerimine, teaduse rahastamine, et oleks võimalik arendada uusi teenuseid ja tooteid, mida rahvusvahelisel areenil presenteerida.

6 Privaatsuskaitse tehnoloogiate rakendamise arendusplaan

6.1 Arendusplaani koostamise metoodika

Intervjuude analüüs. Uuringu käigus viisime läbi intervjuud ning uurisime, millist väärtust looksid andmepõhised teenused ja privaatsuskaitse tehnoloogiad nii Eesti inimestele, ettevõtetele kui ka intervjueeritavatele organisatsioonile.

Intervjuude käigus arutasime ka privaatsuskaitse tehnoloogiate uuringu aruandes kirjeldatud tehnoloogiaid ja nende üldiseid kasutusjuhtumeid. Intervjueeritavad tõid välja, millistest tehnoloogiatest ja rakendustest nad on eriti huvitatud ning millist väärtust nad neis näeksid.

Detailide lisamine ja lünkade täitmine. Esmase teekaardi projektide nimekirja peal tegime järgmised sammud.

1. Jagasime projektid süsteemi ehitamise kontseptsiooni aruandes ([7], pt 3) toodud elutsükli alusel etappideks.
2. Seal, kus tehnoloogiate küpsus on madal või tuleb tehnoloogilise riske kahandada, lisasime teadus-arendusprojekte, millega vastav küpsus luua.
3. Lisasime ka uuringuid ja koolitusi, mis aitavad privaatsuskaitse tehnoloogiate alal teadmust tõsta.

Eelarvestamine. Hindasime, et kõiki projekte paralleelselt teha ei saa ning projektid on omavahel ka järjestuse mõttes sõltuvuses.

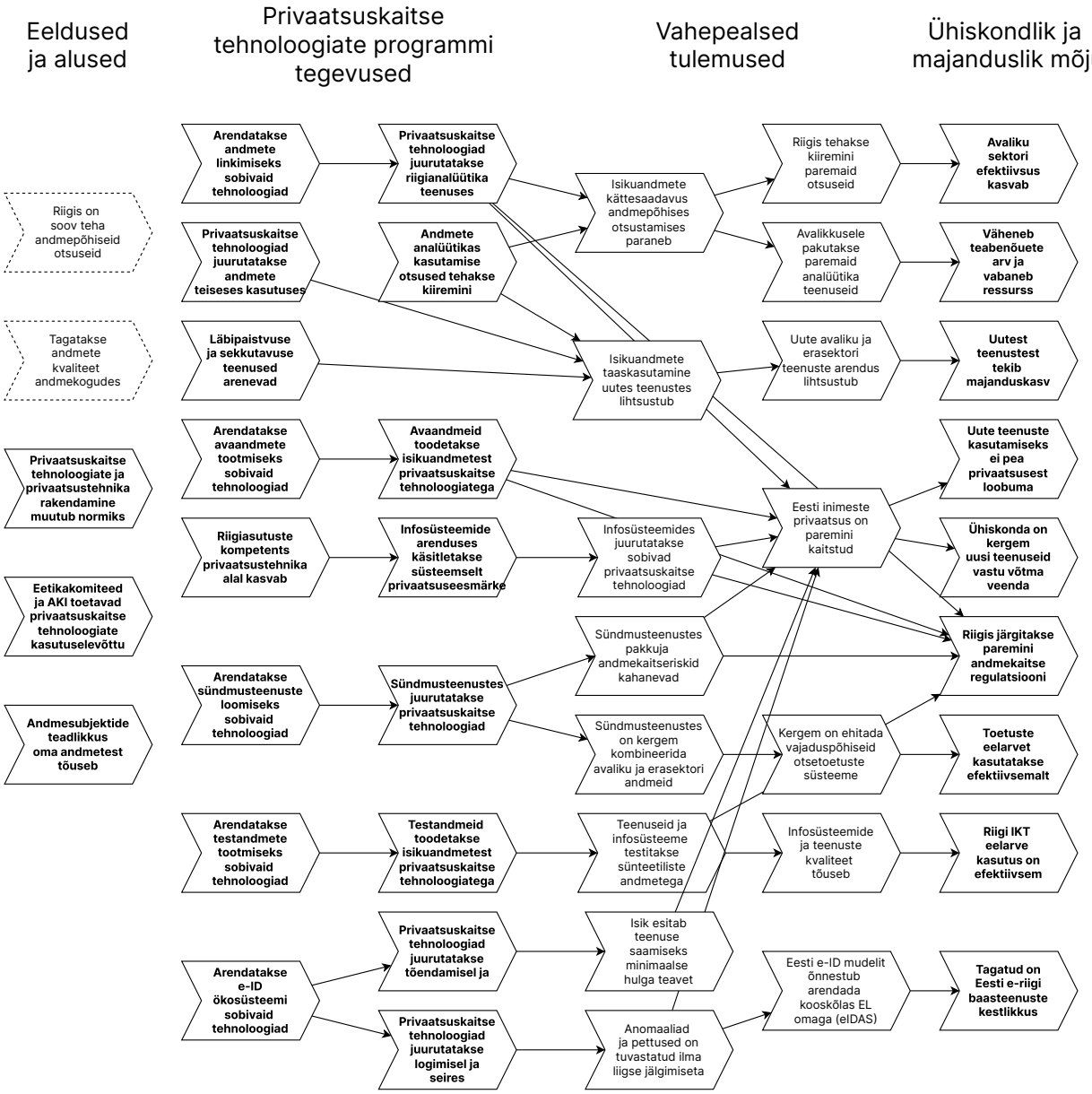
Eraldame teekaardis prioriteedid, millega Eesti võiks tegelema hakata kohe ja millel oleks ka kiirelt saabuv mõju.

6.2 Privaatsuskaitse tehnoloogiate majanduslikud ja ühiskondlikud mõjud

Intervjuude käigus pöörasime eraldi tähelepanu sellele, kuidas läheb elu Eestis paremaks, kui privaatsuskaitse tehnoloogiaid rakendataks. Tegime nendest mõttekäikudest kokkuvõtted, analüüsisime neid ning eraldasime väärtusloome ahelad. Tulem on esitatud Joonisel 1.

Privaatsuskaitse tehnoloogiate mõju avaldub ennekõike andmepõhiste teenuste, infosüsteemide arenduse ning digitaalse identiteedi ökosüsteemide kaudu. Võib öelda, et privaatsuskaitse tehnoloogiad aitavad neid suundi võimendada ning nende täieliku majandusliku mõjuni jõuda. Lisaks on privaatsuskaitse tehnoloogiate juurutamisel ka väga tugev ühiskondlik mõju, sest aidatakse tagada isiku õiguste kaitset, tugevdada ühiskonna usaldust e-riigi vastu ning parandada õigusnormide täitmist.

Intervjuudes mainiti ennekõike andmeanalüütikaga ja pisut vähem digitaalse identiteediga seotud väärtuseid ning seotud vajadusi. Sideandmete kaitse vajadust intervjuus ei mainitud rohkem kui Euroopas menetluses oleva elektroonilise side privaatsuse (ePrivacy) direktiiviga seoses.



Joonis 1. Privaatsuskaitse tehnoloogiate juurutamise eeldused ja mõjud

Paljudes intervjuudes toodi välja paremate otsuste tegemise tähtsust. Uurisime lähemalt, milline on paremate andmete pealt tehtud otsuste toime. Tabelis 1 on näited riigi valdkondadest, kus isikuandmete senisest laialdasemast töötlemisest oodatakse positiivset majanduslikku ja ühiskondlikku mõju.

6.3 Andmepõhine riigivalitsemine ja andmete taaskasutus

Andmepõhine riigivalitsemine ja andmete taaskasutus on Eesti digiühiskonna arengukavas [3] välja toodud kui üks arenguhüppe suundadest. Selle all on konkreetse tegevusena ette nähtud ka privaatsuskaitse tehnoloogiate riikliku programmi elluviimine.

Selle teema all näeme kolme suurt arendusteemat.

6.3.1 Personaliseeritud (sündmus)teenuste platvorm

Motivatsioon. Selleks, et vähendada Eesti inimese jaoks bürokraatiat, toob sündmusteenus kokku andmed teenuse saaja kohta. Selle käigus võidakse koguda mitut sorti isikuandmeid, sealhulgas eriliigilisi, näiteks terviseseisundit puudutavaid andmeid (näiteks lapseootel olek). Selliste andmete koondamine suurel hulgal üle riigi andmekogude tõstab sündmusteenuse privaatsusriski ning seda saab privaatsuskaitse tehnoloogiatega kahandada.

Sündmusteenused võiksid aga teha ka suure sammu edasi ning kaasata andmeid ka erasektorilt. Neist võiks olla kasu nii toetuste määramisel, krediidiotsuste tegemisel kui ka personaalmeditsiinis. Erasektori andmed võivad aga sisaldada ärisaladust ning seega vajada samuti kõrget kaitset, mida privaatsuskaitse tehnoloogiatega saab pakkuda. Tõenäoliselt lihtsaim lahendus oleks juurutada usaldatavate käivituskeskkondade tehnoloogiat.

Personaliseeritud teenustest saadav lisaväärtus.

1. Isikule pakutakse täpsemat teenust tema enda andmete pealt, mis on kokku kogutud ilma tema lisapingutuseta üle e-riigi ning vajadusel ka erasektorist.
2. Täpsemate lähteandmete tõttu saab riik kokkuhoidu vajaduspõhiste otsetoetuste (nt energiatoetuste) pealt.
3. Ühtse turvalise lahenduse leidmisel saavad vastavad teenused edaspidi kiiremini loodud ka siis, kui andmekaitserežiim on keeruline. Väheneb kriitika, mis süüdistab teenuste ehitamata jätmises, ”kuigi riigil on kõik andmed olemas”.
4. Sündmusteenuste osutamise automatiseerimine vähendab avaliku sektori menetluskulusid ja võib samas tõsta poliitikast kasu saavate kodanike arvu.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Täiendava turvalisusega muutub kergemaks erasektori andmete kaasamine.
2. Minimeeritakse sündmusteenuse osutaja töödeldavate isikuandmete mahtu.
3. Andmete koondamiseks üle mitme andmekogu on rakendatud tugevaid kaitsemeetmeid.
4. Arhitektuuri abil saab parandada isikuandmete kaitset ka erasektori teenustes (nt personaalmeditsiin, krediidiregister).

Arenduse sammud.

Valdkond	Andmete kasutus	Oodatav mõju
Statistika	Elanike jaotus piirkondades	Paremini korraldatud kohalike omavalitsuste teenused
	Teave leibkondade toimetuleku kohta	Erasektor teeb paremaid otsused, näiteks pangad krediidipoliitika osas
Õigus	Kriminaalpoliitika valdkonnaga seotud andmete analüüs	Taasühiskonnastamise programmid on efektiivsemad, ohvrite elu paraneb
Rahva tervis ja sotsiaalvaldkond	Ravitulemuste ja ravikulude info ühendamine ja analüüs	Parendussammud ravi rahastamises ning efektiivsem tervishoiusüsteem, mis tõstab tervena elatud ja töötatud aastate arvu
	Leibkondade koosseisu analüüs	Tervishoiu teenuste vajaduse ennustamine ning parem investeeringute efektiivsus
	Tervishoiu edenduse meetmete analüüs	Selgub, millised meetmed vananevas ühiskonnas tegelikult efekti annavad ja millesse on otstarbekas investeerida, kasvab tervena elatud ja nt töötatud aastate arv
	Avaliku ja erasektori raviarvete analüüs	Avastatakse paremini pettuseid ravikulude raporteerimisel
Sisekaitse	Inimeste elukohaandmete ja elamufondi analüüs	Päästestrateegia uuendamine et muuta päästeressursside paigutust ning vabatahtlikele vahendite jagamist
Transport	Liiklusõnnetuste analüütika üle andmekogude	Õnnetuste põhjuste parem mõistmine ning efektiivsem ennetus, väiksem kahju tervisele ja varale.
Rahandus	Krediiditeabe koondamine üle erasektori pakkujate	Vastutustundliku laenamise põhimõtete jõustamine ning turu korrastamine
	Pensionifondide mahu ja efektiivsuse analüütika üle teenusepakkujate	Pensionipoliitikat planeeritakse efektiivsemalt ning riigi jaoks säästlikumalt
	Laiapõhjaline majandusandmete (maksud, toetused, pensionid, import, eksport jne) ühendamine ja analüüs	Fiskaalpoliitika mõjuanalüüside kvaliteet tõuseb ning eelarve ennustatavus paraneb
	Inimeste liikumisinfo analüüs (eriti üle piiride)	Rändeprognoosid ja sellega seotud majandusprognoosid on täpsemad

Tabel 1. Valdkonnaspetsiifilised oodatud mõjud isikuandmete laialdasemal töötlemisest

1. **Esimene samm: innovatsiooniprojekt.** Projekt leiab sobiva tehnilise lahenduse isikule privaatsust säilitava teenuse pakkumiseks. Võiks olla võimalik teostada Riigikantselei vastava meetme kaudu. Tulemiks on privaatsuskaitse tehnoloogiaid rakendav arhitektuur ja

prototüüp.

2. **Teine samm: pilootprojekt.** Luuakse esimene teenus. Valitakse üks akuutne teema (näiteks mõne toetuse määramine) ning ehitatakse valmis esimene teostus, saavutades kiiresti majandusliku efekti. Tulemiks on üks juurutatud ja kasutatud pilootteenus.
3. **Kolmas samm: platvormi loomine ning laienemine.** Tehnoloogiline lahendus muudetakse korduvkasutatavaks ning selle platvormi peale ehitatakse järgmised teenused ning saavutatakse taaskasutuse võimekus.

6.3.2 Andmekogudeülese analüütika lahendus

Motivatsioon. Andmetepõhine juhtimine ja otsustamine saab toimida siis, kui vajalikud andmed ja analüüsid on olemas ja värsked. Nii saab hinnata võimalike uute poliitikate mõju rahandus-, tervishoiu-, sotsiaalpoliitikas, õigus- ja sisekaitses ning teha poliitikat toetavaid ennustusi. Samamoodi saab analüütikaga leida pettuseid olemasolevate poliitikate rakendamisel, eriti kui ühe organisatsiooni vaatest väärkasutus välja ei tule. Mõlemal juhul on efekti saamiseks vaja ühendada ja analüüsida mitut andmekogu, mis isikustatud andmete puhul võib teatud juhtudel tähendada massandmetöötlust ja/või kõrgendatud riski, näiteks andmete lekkimisel.

Poliitikauuringutel on oluline ajaline faktor – küsimusele vastust on vaja lühikese etteteatamisega. Uue analüütikaprojekti algatamine ning läbiviimine on aeganõudev. Ühekordsete analüüside asemele on vaja püsivat andmete linkimise võimega infosüsteemi, mille tulemid oleksid pidevalt ajakohased. Privaatsuskaitse tehnoloogiad tuleks valida lähtuvalt talitluse analüüsist.

Andmekogudeülesest analüütikast saadav lisaväärtus.

1. Paremini motiveeritud ja täpsemalt ette valmistatud poliitikamuutus säästab riigi ressursse.
2. Poliitika andmepõhine mõjuanalüüs on efektiivsem, kui kaasab mitme valdkonna vaadet. Näiteks tervishoiu puhul on avaliku ning eratervishoiu tervikuna käsitlemine informatiivsem kui eraldiseisvalt.
3. Transpordis ja sisekaitses tähendab laiem vaade õnnetustele või näiteks tulekahjude andmete töötlemine efektiivsemat ennetust.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Mitmest andmekogust paljude isikute andmete koondamisel ja ühendamisel tõuseb isikute kohta lekkida võiva teabe hulk märgatavalt ning privaatsuskaitse tehnoloogiad on selle ohu kahandamiseks täpselt mõeldud lisameetmed.
2. Mõned privaatsuskaitse tehnoloogiad aitavad jälgida, et loodavatele süsteemile ei lisataks algses ülesandepüstituse ette nägemata ning soovimatuid rakendusi.

Arenduse sammud.

1. **Esimene samm: innovatsiooniprojekt.** Väga paindlikku analüüsivõimekust pakkuvad privaatsuskaitse tehnoloogiad on madalama tehnoloogia küpsustasemega kui need, millega saaks konkreetset sündmusteenust pakkuda. Esimese TA projektiga tuleb leida tasakaal vajalike uuringute paindlikkuse, nende läbiviimiseks soovitavate töövahendite ning nõuetele vastavate privaatsuskaitse tehnoloogiate vahel. Lisaks tuleb selle projekti käigus lahendada ka õiguslik käsitlus andmekoguüleste analüüside läbiviimiseks privaatsuskaitse tehnoloo-

giatega. Tulemiks on arhitektuur ja õiguslik mudel poliitikaanalüüsi andmeteenusele.

2. **Teine samm: pilootprojekt.** Tuginedes esimese sammu tulemusele teostatakse esimene korduvkasutatav sobivaid privaatsuskaitse tehnoloogiaid rakendav poliitikaanalüüsi teenus. Pilootprojekti partner tuleb valida valdkonnast, kus nähakse suurimat paremast planeerimisest tulenevat säästuvõimalust. Tulemiks on juurutatud analüüsiteenus.
3. **Kolmas samm: platvormi loomine ning laienemine.** Leitakse järgmised kasutajad (nt ministeeriumid) ning tehnoloogiline lahendus laiendatakse vastavalt nende vajadusele. Luuakse taaskasutatavad teenused. Tulemiks on uued analüüsiteenused samal arhitektuuril.

6.3.3 Madala taasisikustamise riskiga avaandmete tootmine

Motivatsioon. Avaandmed aitavad innovatsiooni kaasata ühiskonda laiemalt. Ettevõtted, teadlased ja õppeasutused saavad avaandmetest toota uusi teadmisi, mudeleid ja teenuseid. Mitteisikustatud andmetest avaandmete tootmine on lahendatud probleem, kuid isikustatavatest andmetest avaandmete tootmiseks on tehnoloogiline küpsus Eestis veel madal.

Avaandmete iseloomust lähtuvalt on nende töötlemine piiramata ning avaldaja ei saa ka kontrollida, milliste täiendavate andmetega neid kombineeritakse. Sellest lähtuvalt on kõrge risk, et nõrgalt anonüümitud andmeid saab teiste andmetega ühendades isikustada ja ühendada. Nii võib avaandmete kaudu tekkida lubamatu isikuandmete töötlus. Selle probleemi lahendamiseks on olemas sobivad privaatsuskaitse tehnoloogiad[50]. Kasu võiks olla diferentsiaalprivaatsusest, sünteetiliste andmete genereerimisest või tugevatest anonüümise tehnoloogiatest.

Isikutest lähtuvatest avaandmetest saadav lisaväärtus.

1. Isikustatavad andmed nagu terviseandmed, energia tarbimise andmed või ka finantssektori andmed on seni jäänud innovatsioonis rakendamata ning seega pole nendest tuletatav ühiskondlik ja majanduslik mõju ilmneda saanud.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Privaatsuskaitse tehnoloogiatel on olemas konkreetsed tööriistad, meetodid ja mõõtemeetodid andmete anonüümimise meetodite kasulikkuse ja saavutatava anonüümsuse võrdlemiseks.
2. Sobivate privaatsuskaitse tehnoloogiate rakendamisel saab kaitsta avaandmeid ka pikema perioodi jooksul tekkiva isikute taasidentifitseerimise ründe vastu.

Arenduse sammud.

1. **Esimene samm: väikesed pilootprojektid.** Lähtuvalt rahvusvahelisest kogemusest ja tehnoloogiate küpsusest saab siin alustada kohe pilootprojektidega, mis kontrolliks erinevate tehnoloogiate sobivust konkreetseteks ülesanneteks.
2. **Teine samm: teadmuse koondamine ja jagatud teenuse loomine.** Tuginedes pilootprojektide kogemustele saab hakata teadmust koondama ja süstematiseerima. Teises etapis võib ka teostada avaandmete tootmise mitmest andmekogust lingitud andmetel, luues selleks teenuse mudelid, mis teevad linkimist vastavate privaatsuskaitse tehnoloogiatega.

[50] Mõnede andmete (geeniandmed, liikuvusandmed) puhul on avaandmeteks muutmine tänase teadmuse juures võimatu, sest nende andmete puhul on kirje unikaalsus liiga suur.

6.4 Tulevikukindlad digiriigi platvormid

Teine digiühiskonna arengukavas [3] välja toodud arengusuund on e-riigi platvormide tulevikukindlus. X-tee, riigi digitaalne identiteet ja portaalid on Eesti igapäevaelu tähtsad osad ning vajavad pidevat kaasajastamist. Lähtuvalt andmekaitse arengust Euroopas on privaatsuskaitse tehnoloogiad samuti meie alusplatvormide teekaardil.

6.4.1 Privaatsuse kaitse lahendused digitaalse identiteedi opereerimisel

Motivatsioon. Toimiv digitaalse identiteedi ökosüsteem vajab kehtivuse kinnituse teenust, et vältida võltsitud või tühistatud identiteetide kasutamist. Identiteedi pakkujad ja vahendajad käitavad ka logimisteenuseid, et leida vigu ja tuvastada pettuseid või anomaaliaid. Nende teenuste osutamisel tekkivad logid on digitaalses ühiskonnas osaleja profiiliks ning annavad mõista, milliseid teenuseid keegi kasutab ning kuskohas ta sellel ajal on. Mida rohkem inimene digitaalset identiteeti kasutab, seda paremini avaldab sellise logi aegrida infot isiku liikumiste kohta.

Privaatsuskaitse tehnoloogiatega saab luua digitaalse identiteedi ökosüsteemis teenuseid, mis väldivad isiku profileerimist avaliku ja erasektori teenusepakkujate poolt. Siiski saab säilitada võimaluse leida mustreid ja pakkuda kasutajatuge.

Digitaalse identiteedi ökosüsteemi teenuste lisaväärtus.

1. Digitaalse identiteedi kehtivuskinnitus on Eesti eID põhiosa selle algusest peale. Ilma selleta oleks võimalikud samasugused ründed nagu näiteks Euroopa COVID-19 vaktsineerimistõenditega, kus leidus kehtivaid tõendeid surnud inimestele ja väljamõeldud animafilmitegelastele.
2. Digitaalse identiteedi pakkujate ja vahendajate jaoks on logid töökindluse tagamiseks ja pettuste tuvastamiseks peamine töövahend.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Privaatsuskaitse tehnoloogiate rakendamine logimisel vähendab nii avaliku kui erasektori teenusepakkujate võimekust koostada identiteedi kasutajate liikumise ja harjumuste profiil.
2. Euroopa Liidu uued õiguslikud algatused (näiteks eIDAS 2.0) võivad andmekaitse argumentidega digitaalse identiteedi (nt kukrute) kasutamise korda tõsiselt muuta. Sellises olukorras peab Eesti olema vajadusel valmis näitama, kuidas eID opereerimisel liigset profileerimist välditakse.

Arenduse sammud.

1. **Esimene samm: juriidilised ja tehnoloogilised alusuuringud.** Digitaalse identiteedi ökosüsteemi osapoolte ja õigusekspertidega koos leitakse sobivad privaatsuskaitse tehnoloogiad, mis tagavad teenuse kasutamisel vigade tuvastamise ning pettuste vältimise nii, et profileerimise risk on võimalikult madal.
2. **Teine samm: analüüsi ja arhitektuuri koostamine.** Tuginedes alusuuringute tulemusele kavandatakse privaatsuskaitse tehnoloogiaid rakendavad tehnilised lahendused avaliku sektori eID teenuse pakkujatele ning vahendajatele.
3. **Kolmas samm: teostus.** Sobivate privaatsuskaitse tehnoloogiate abil teostatakse kavandatud süsteem.

6.4.2 Privaatsust säilitavad tõestused

Motivatsioon. Täna tehakse Eestis nii füüsilise kui digitaalse identiteedi vahenditega mitmeid tõestuseid. Näiteks poes saab enda vanust tõestada isikutunnistust näidates. Selle käigus aga esitatakse müüjale terve isikukood, ehk rohkem teavet, kui müüjal on toimingu teostamiseks vaja. Olukord muutub veelgi keerukamaks kukrute puhul, kus tõestuste esitamine on peamine kasutusjuhtum. Ka siin on oht, et tõestamise akti käigus antakse üle liiga palju teavet, mida saaks minimeerida nii, et tõestuse vastuvõtja saab otsuse teha, kuid ei näe liiasusega andmeid.

Praktikas näeks see välja näiteks nii, et mõne järgmise põlvkonna isikutunnistuse või mobiiltelefonis oleva kukruga saab viipemakse terminali abil müüjale tõestada, et ostja on näiteks 18-aastane või vanem. Privaatsuskaitse tehnoloogiate abil saab teha ka keerukamaid tõestuseid, näiteks kuulumist mingisse gruppi või isikuandmete vastavust mõnele normile (nt terviseloo vastavus tervisenõuetele). Võtmetehnoloogiaks võiks osutuda lihtsamad (nt vanusevahemiku tõestamiseks) või keerukamad (nõuetele vastavuse tõestamiseks) nullteadmustõestused.

Tõestuste ökosüsteemi loodav lisaväärtus.

1. Enda identiteedi kohta tunnuste (õigused, tunnistusd, lojaalsusprogrammid, kuuluvused) tõestamine on igapäevane äriprotsessi osa. Selle digitaliseerimisest saab protsess efektiivsemaks minna.
2. Tõestuste esitamise väärtus avaldub lõpuks eriti võimsalt piiriüleses asjaajamises, kus loodetavasti lihtsustub vähemalt Euroopa Liidu piires õppetulemuste, erinevate lubade, äritegevuse ja hangete käigus tõestust ristkasutus. Selle käigus on aga minimeerimisel kindlasti tähtis roll, et vältida üleliigset piiriülest andmetöötlust.
3. Digitaalse identiteedi pakkujate ja vahendajate jaoks on logid töökindluse tagamise ja pettuste tuvastamiseks peamine töövahend.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Privaatsuskaitse tehnoloogiatega saab tõestusi tehes minimeerida isikustatud andmete ülekande vajadust osapoolte tõestaja ja tõestuse kontrollija vahel.
2. Tõestuse kontrollijal ei ole vaja tõestuse andmete kontrollimiseks teha järelepärimisi registritesse – lähteandmetest tehtud tõestuse saab teha tõestuse osana.

Arenduse sammud.

1. **Teadus-arendusprojekt.** Tehnoloogia küpsus on veel madal, seega on esimeseks sammuks vastavasisulised teadusuuringud.

6.5 Keskselt osutatud IT-alusteenused

E-riigi arenduse käigus on tähtis hallata uute süsteemide loomisel tekkivat keerukust ning luua keskseid teenuseid, mis aitavad tagada ühtset kvaliteeti ning jagada ressursse. Privaatsuskaitse tehnoloogiate kasutuselevõtul on samuti tähtis tehniliste lahenduste jagamine, millega väheneb tehnoloogia rakendamise kulu süsteemi kohta.

6.5.1 Sünteetiline e-riigi kaksik testimiseks

Motivatsioon. Infosüsteemide ja teenuste testimisel on vaja andmeid. Isikuandmeid töötlevates süsteemides aga ei ole isikuandmetega testimine lubatud. Olukord on veelgi keerulisem, kui arenduse või testimise teenus on hankega sisse ostetud.

Lahendust nähakse sünteetilistes andmetes, mille toel ehitatakse üles sünteetiline digitaalne teisik – testkeskkond, kus töötavad X-tee teenused, kuid milles kõik andmed on juhuslikult sünteesitud isikute kohta, keda tegelikult olemas ei ole. Sellise testkeskkonna abil saab testida uusi infosüsteeme, mis vajavad integratsioone mitmete seotud süsteemidega. Privaatsuskaitse tehnoloogiate abil saab tõsta sünteetiliste andmebaaside kvaliteeti, koostades need pärisandmete pealt arvutatud mudelitest. Kasu võiks olla näiteks sünteetiliste andmete genereerimisest.

Sünteetiliste testandmete keskkonna lisaväärtus.

1. Infosüsteeme ja teenuseid saab testida andmetega, mis ei ole isikustatavad (sest vastavaid isikuid ei ole olemas, nad on välja mõeldud).
2. Sünteetilisi andmeid saab testimiseks anda ka lepingulistele arenduspartneritele.
3. Kui testkeskkond on keskne teenus, mida saavad kasutada mitmete riigiasutuste teenuste arendajad, säästetakse ka kõigi jaoks ressurssi, igaüks ei pea sünteesima oma kunstlikku rahvastikuregistrit.

Privaatsuskaitse tehnoloogiatest tulenev lisaväärtus.

1. Privaatsuskaitse tehnoloogiatega saab tõsta sünteetiliste testandmete kvaliteeti, eriti kui need sünteesida lähteandmete modelleerimise baasil.
2. Privaatsuskaitse tehnoloogiatega saab ka kaitsta lähteandmetest sünteesimudelite tootmist ning selleks vajalikku andmete ühendamist.

Arenduse sammud.

1. **Esimene samm: eelanalüüs** Viie riigiasutuse testimisvajaduse analüüsile toetudes koostatakse e-riigi testkeskkonna talitluse mudel.
2. **Teine samm: tehnoloogiate valik ja arhitektuur.** Talitluse mudelite põhjal leitakse sobivad andmete sünteesi tehnikad ning protsessid sünteetiliste andmebaaside uuendamiseks kui teenused uuenevad. Valmib testkeskkonna arhitektuur.
3. **Kolmas samm: testkeskkonna pilootprojekt.** Arendatakse välja testkeskkonna pilootprojekt, mis võimaldab kahel asutusel testida mõnda nende süsteemi ja integreerib selleks vastavad teenused.
4. **Neljas samm: uute andmekogude integreerimine.** Testkeskkonda hakatakse kasutama veel kümne infosüsteemi või teenuse arendamisel ja testimisel

6.5.2 Teised perspektiivsed projektid

Keskselt pakutava privaatsuskaitse tööriistakasti arendus. Infosüsteemide, sündmusteenuste, Bürokrati jt krattide arenduse käigus tuvastatakse kindlasti veel korduvaid vajadusi, mida privaatsuskaitse tehnoloogiatega lahendada. Heaks näiteks on RIA arendatav tekstist identifitseerivate osade tuvastamise ja eraldamise teenus. Sarnaseid süsteeme tuleks keskselt hallata

ning nende kohta teadmust levitada, vajaduse koolitusi tehes. Korduvkasutus vähendab lahenduste dubleerimist ning kulusid tehnoloogiate arendamisele.

6.6 Uute lähenemisviiside pidev katsetamine

Mõned infosüsteemid või teenused on erilised ning saaksid uutest lähenemisviisidest rohkem kasu kui teised. Toome siin välja mõned intervjuudest välja tulnud ideed, kus privaatsuskaitse tehnoloogiast tõuseks märkimisväärne lisaväärtus. Märgime ka ära, et tehnoloogiad, mis olid kunagi uued, võivadki saada ühel hetkel normiks. Hea näide on turvalise internetiside protokoll TLS, mis on tänapäeval kasutusel pea kogu internetiside kaitsel. TLS levikule andsid tugeva tõuke muuhulgas ka Edward Snowdeni lekitatud materjalid riiklike jälgimisprogrammide kohta [51].

Privaatsust säilitav kratiseansi klassifitseerija ja marsruutija pilootprojekt. Bürokrati kasutusmugavuse üks võtmeelement on ühetaolisus – kodaniku jaoks on Bürokratiga suhtlemiseks üks aken ning ta ei pea valima, kellega ta suhtleb. Selleks, et tema sõnumite saajad ei peaks töötlema isikuandmeid, mis ei ole neile ette nähtud (ning on näiteks märkimisväärselt kõrgema riskiga), on vaja sõnumeid klassifitseerida. Sel otstarbel saaks kasutada privaatsuskaitse tehnoloogiad (näiteks usaldatavaid käivituskeskkondi).

Privaatsuskaitse tehnoloogiatele toetuvad andmesaatkonnad. Andmesaatkonnad talletavad varukoopiaid Eesti e-riigi süsteemidest, et neist süsteemid vajadusel taastada. Perspektiivselt saaks turvalisest ühisarvutusest inspireeritud privaatsuskaitse tehnoloogiaid rakendada selleks, et varukoopia taastamiseks oleks vaja näiteks suvalise kahe või kolme saatkonna koostööd ja nõusolekut. Nii ei oleks näiteks ühe saatkonna käes olevate võtmete lekkimine koheselt risk Eesti e-riigi varukoopiatele. Alustada tuleks talitluse analüüsiprojektist, tehnoloogiad võtmete jagamiseks ja kaitseks oleks lihtsad ning analoogsed Smart-ID teenuses kasutatavatega.

Privaatsuskaitse tehnoloogiate kasutamine eriliigiliste isikuandmete töötlemisel mitte-Euroopa andmekeskustes ja pilves. Täna ei ole kindlust, et pikas perspektiivis on Euroopast väljaspool kasutatavates andmekeskustes võimalik töödelda Euroopa kodanike eriliigilisi isikuandmeid, näiteks terviseandmeid. Uusi andmekaitse adekvaatsuse leppeid sõlmitakse (näiteks Ameerika Ühendriikidega), kuid varasema kogemuse põhjal võivad need ka õigustühiseks osutuda. Digitaalse suveräänsuse ja õiguskindluse tagamiseks on otstarbekas algatada teadus-arendusprogramme, mis uuriks, milliseid pilvteenuseid oleks võimalik kasutada ka ilma adekvaatsusotsuseta, kui lisanduva turvameetmena kasutada privaatsuskaitse tehnoloogiaid. Selle lähenemise lubavust toetab Euroopa Andmekaitsenõukogu 2020. aasta novembri soovitus, mis pakub piiriüleseks andmetöötluseks lisanduvate meetmetena mitmeid privaatsuskaitse tehnoloogiaid [21].

Kolmanda osapoole personaalmeditsiini otsusetoe süsteemide ühendamine Eesti terviseandmete külge. Vahel võib riik tahta kaitsta enda inimeste andmeid mõne erasektori partneri eest. Heaks näiteks on personaalmeditsiini teenused, mida võivad opereerida (ka välisriikide) ettevõtted, kuid mis sooviksid taaskasutada Eesti tervise infosüsteemi andmeid. Nõusolekuteenuse abil saab luua selliseks töötlemiseks õigusliku aluse ja privaatsuskaitse tehnoloogiate abil saab vältida nende volitamata kasutust kolmanda osapoole teenuses. Eraldi keerukus tekib juhul, kui soovitakse teostada tulevikus sõeluuringuid näiteks harvikhaiguste kohta. Andmepõhiseid sõe-

[51] Looking back at the Snowden revelations. Matthew Green. https://blog.cryptographyengineering.com/2019/09/24/looking-back-at-the-snowden-revelations/ (Viimati külastatud 3. märtsil 2023).

luuringuid saaks teha kogu vastava populatsiooni andmete peal, aga sellisel juhul nõusolekuteenus ei aitaks ja privaatsuskaitse tehnoloogiate toel tuleks otsusetoesüsteemiga töödelda paljude patsientide andmeid üheaegselt. Lähtuvalt tehnoloogia ja ärimudeli madalast küpsusest tuleks siin alustada teadusuuringutest.

Tehnoloogiad andmete vesimärgistamiseks. Kui Eesti riik väljastab näiteks teadusuuringuteks pseudonüümitud või anonüümitud andmeid, ei saa välistada, et need andmestikud saavad avalikuks kolmandatele osapooltele. Sellisel juhul võivad kannatada Eesti andmete teisese kasutusega seotud ärimudelid. Sellises olukorras oleks mugav, kui iga anonüümimise või diferentsiaalprivaatse avaldamise käigus *vesimärgistataks* andmestik erineva müraga, et hiljem oleks võimalik jälgida, millise koostööpartneri kaudu andmed lekkisid. Sarnaseid (*traitor tracing*) ideid on varem kasutatud nt filmide piraatlevi takistamiseks. Ka siin tuleks alustada teadusuuringust ja jätkata talitluse analüüsiga.

Privaatsuskaitse tehnoloogiad missioonikriitilistes infosüsteemides. Privaatsuskaitse tehnoloogiatega oleks võimalik ehitada paremaid versioone infosüsteemidest, mille rajamist on aastaid planeeritud, kuid mis ei ole veel kavandamise faasist edasi jõudnud. Headeks näideteks on positiivne krediidiregister ja digitaalne majutuskaart. Mõlemal süsteemil on tugev erasektori komponent (krediidiasutused, majutusasjutused), andmed tekiks isiku suhtluses nende ettevõtetega ning riiki huvitaks üldised mustrid (krediidimahtude ja majutujate jaotused). Mõlemal teenusel saaks olla ka tugev läbipaistvuse ja sekkutavuse komponent.

6.7 Avatud innovatsioon ja digiriigi kogukonna arendamine

Materjalide eestindamine. Privaatsustehnika, privaatsuskaitse tehnoloogiate, privaatsuse juhtimise ja privaatsusmõjude analüüsi kompetentsi tõstmiseks soovitame tõlkida eesti keelde järgmised standardid:

1. ISO/IEC 27550 (privaatsustehnika süsteemide elutsüklis)
2. ISO/IEC 29134 (privaatsusmõjude analüüsi metoodika)
3. ISO/IEC 27701 (privaatsuse juhtimine organisatsioonis)

Kompetentside arendus ja praktikate levitamine. Lähtuvalt privaatsuskaitse tehnoloogiate rakendamisest kogutakse kokku juhised ning parimad praktikad ning neid levitatakse koolituste ja materjalidega. Sobivad teemad on:

1. Privaatsuskaitse tehnoloogiate alane koolitus.
2. Privaatsusmõjude analüüsi, pseudonüümimise ja anonüümimise ohtude hinnangud.
3. Koolitada organisatsioone andmejälgija ning nõusolekuteenuse kasutuselevõtu osas ning toetada rakendusprojekte sobiva meetmega.
4. Koolitada organisatsioone uute privaatsuskaitse tehnoloogia platvormide osas ning toetada rakendusprojekte sobiva meetmega.
5. Koolitada organisatsioone avaandmete tootmise metoodika osas.

Jätkuvad uuringud. Privaatsuskaitse tehnoloogiate kontseptsioon ja teekaart vajavad ka edaspidi uuendamist ning jätku-uuringuid, sealhulgas järgmistel teemadel.

1. Lisada E-ITS standardisse privaatsuskaitse tehnoloogiate ning privaatsustehnika kasutamist toetav andmekaitse moodul.
2. Privaatsuskaitse tehnoloogiate taasisikustamise riskide ja meetodite näidiste koostamine andmeteadlastele ja andmekaitsespetsialistidele
3. Privaatsuskaitse tehnoloogiate turu-uuring.

Avalik teavitus. Tähtis osa uute tehnoloogiate vastuvõtul on inimeste reaktsioon. Seega on privaatsuskaitse tehnoloogiate programmi käigus otstarbekas ka paremini teavitada rahvast nende andmete töötlemisest digiriigis ning üldisest andmehügieenist. Inimeste kõrgem teadlikkus nende andmete töötlemise meetoditest toetab ka kodanikuühiskonna rolli riigi järelevalve teostajana.

6.8 Tulemid, mõõdikud ning ajakava

Tegevus	Etapp	Tulemid	Mõõdikud ja sihid	Algus	Võimalik elluviija
Andmepõhine riigivalitsemine ja andmete taaskasutus					
Personaliseeritud (sünd-mus)teenused	Innovatsiooniprojekt	Arhitektuur ja prototüüp	Teenuseid analüüsi kaasatud (5)	2023	Riigikantselei, RIA
Personaliseeritud (sünd-mus)teenused	Pilootprojekt	Juurutatud pilootteenus	Teenuseid teostatud PET abil (1)	2024	RIA
Personaliseeritud (sünd-mus)teenused	Platvormi loomine ja korduvkasutus	X-tee ja e-ID-ga ühilduv platvorm turvaliste äriraken-duste loomiseks	Platvorm PET abil teenus-te teostamiseks (1), Teenu-seid teostatud PET platvor-mi abil (5)	2025+	RIA
Andmekogudeülese analüütika ja poliiti-kauuringud	Innovatsiooniprojekt	Arhitektuur, õiguslik mu-del	Riigiasutusi, kelle nõuded on kaasatud (4)	2024	Riigikantselei
Andmekogudeülese analüütika ja poliiti-kauuringud	Pilootprojekt	Juurutatud analüütika-teenus	Teenuseid teostatud PET abil (1)	2025+	Probleemi omanik, näi-teks Tervise-kassa, TEHIK, Rahandusmi-nisteerium, RMIT
Andmekogudeülese analüütika ja poliiti-kauuringud	Platvormi loomine	X-teega ühilduv plat-vorm poliitikauuringu-teks ja ennustusteks	Platvorm teostatud PET abil (1)	2025+	RIA

Andmekogudeülese analüütika ja poliitikauuringud	Platvormi rakendamine asutustes	Platvormi toel ehitatakse valmis konkreetsete osapoolte andmevood ja poliitikaanalüüsi süsteemid	Riigiasutusi, kellele on loodud PET abil poliitikaanalüüsi võimekus (4)	2025+	Probleemide omanikud
Madala taasisikustamise riskiga avaandmete tootmine	Pilootprojektid	Kolm asutust on enda andmestiku	Organisatsioone, kes on avaandmeid tootnud PETide abil (3), taasidentifitseerimise riski analüüsid teostatud (3)	2023-2024	Kandidaadid: TEHIK, Tervisekassa, Päästeamet
Madala taasisikustamise riskiga avaandmete tootmine	Taaskasutatavate lahenduste loomine ja rakendamine	Taaskasutatav avaandmete tootmise tööriistakast	Avaandmete töötlemise tööriistakast valmis (1), uued organisatsioonid on seda kasutanud avaandmete tootmiseks (3)	2024	Kandidaadid: Transpordiamet, SMIT, PPA
Tulevikukindlad digiriigi platvormid					
Privaatsuse kaitse lahendused digitaalse identiteedi opereerimisel	Innovatsiooniprojekt	Tehnoloogiad, õiguslik mudel, prototüüp	Leitud on PETid, mis lubavad logimist pettuste tuvastust ja töökindluse tagamist eID logides ja teenustes (1)	2023	Riigikantselei ja/või RIA
Privaatsuse kaitse lahendused digitaalse identiteedi opereerimisel	Analüüs ja arhitektuur	Arhitektuur ja talitlus teada	eID teenuse kehtivuskinnituste või logimise teenus jaoks on olemas PET kasutav arhitektuur (1)	2024	RIA
Privaatsuse kaitse lahendused digitaalse identiteedi opereerimisel	Teostus	Teostus ühes teenuses	eID teenuse kehtivuskinnituste või logimise teenus jaoks on olemas PET kasutav teostus (1)	2025+	RIA

Privaatsust säilitavad tõestused	Innovatsiooniprojekt	Kaardistatud on sobivad tehnoloogiad uute eID kasutusmudelite jaoks	Teada on tuleviku eID tõestust kasutusmudelid ning nendeks sobivad PETid (3)	2025+	Riigikantselei ja/või ETAG
Keskselt osutatud IT-alusteenused					
Sünteetiline e-riigi kaksik testimiseks	Talitluse eelanalüüs	Testkeskkonna talitlusmudelid on kavandatud	Riigiasutused, kelle nõuded on kaasatud sünteetiliste andmetega testkeskkonna loomisel (5)	2023	RIK
Sünteetiline e-riigi kaksik testimiseks	Innovatsiooniprojekt	Arhitektuur ja tehnoloogiate valik	Leitud on sünteetilise e-riigi kaksiku loomiseks sobivad PETid (1) ja nende baasilt on koostatud lahenduse arhitektuur (1)	2024	RIK
Sünteetiline e-riigi kaksik testimiseks	Pilootprojekt	X-tee testkeskkond, kahe pilootandmekogu sünteetiline kaksik	Loodud on X-tee teenuste testkeskkond (1) ning selle peal on integreeritud andmekogude sünteetilised kaksikud et (2) asutust saaks oma süsteeme testida uues keskkonnas	2024	RMIT, RIK
Sünteetiline e-riigi kaksik testimiseks	Keskkonna rakendamine asutustes	10 andmekogu sünteetilised teisikud on testkeskkonda kaasatud	Testkeskkonda on hakanud kasutama (10) infosüsteemi testimiseks	2025+	TEHIK, SMIT, FI, RMIT
Keskselt pakutava privaatsuskaitse tööriistakasti arendus	Tööriistade arendus	Korduvkasutatav lahendused on olemas ning teadmus levib	Jagatud privaatsuskaitse tehnoloogiate tööriistakasti kasutavad (10) teenust või infosüsteemi	2025+	RIA
Uute lähenemisviiside pidev katsetamine					

Privaatsust säilitav kratiseansi klassifitseerija ja marsruutija pilootprojekt	Analüüs ja arendus	Klassifitseerija on juurutatud.	100% Bürokrati sessioonidest kasutavad privaatsuskaitse tehnoloogiatel põhinevat klassifitseerijat.	2023	RIA
Privaatsuskaitse tehnoloogiatele toetuvad andmesaatkonnad	Analüüs ja arendus	Andmesaatkondade krüptograafiliste võtmete hajus haldus on juurutatud	Ükski (0) andmesaatkond ei suuda üksi varukoopiaid taastada ning vaba selleks vähemalt 1 või 2 teise andmesaatkonna koostööd.	2025+	RIA
Privaatsuskaitse tehnoloogiate kasutamine eriliigiliste isikuandmete töötlemisel mitte-Euroopa andmekeskustes ja pilves	Innovatsiooniprojekt	Lahendused pilvandmetöötluse rakendamiseks nt terviseandmetega	Eestil on võimekus rakendada piiriülesel isikuandmete vahetusel vähemalt (3) privaatsuskaitse tehnoloogiat	2025+	Riigikantselei ja/või ETAG
Kolmanda osapoole personaalmeditsiini otsusetoe süsteemide ühendamine Eesti terviseandmete külge	Innovatsiooniprojekt	Tehnoloogiad on valitud ja talitlusmallid on koostatud	(2) erasektori otsustoe süsteemi kasutavad andmeid patsiendi digiloost.	2025+	RIA
Avaandmete vesimärgistamise tehnoloogia lekete allikate tuvastamiseks	Teadusprojekt	Talitlusmudel andmete avaldamisest nii, et lekked on jälitatavad.	(1) asutus on avaldatud andmete vesimärgistamist piloteerimas	2025+	ETAG

Positiivse krediidiregistriga seotud isiku krediidikonto portaal	Isik saab ülevaate enda kõigist krediidikohustustest ning talle pakutakse täpsetelt andmetelt personaalse krediidinõustamise teenust	Positiivse krediidiregistri arhitektuur ja teostus kasutavad privaatsuskaitse tehnoloogiaid, et tasakaalustada isikute, erasektori krediidiasutuste huvisid ja riigi krediidipoliitikat	(1) privaatsuskaitse tehnoloogiaid rakendav positiivne krediidiregister on juurutatud	2025+	
Avatud innovatsioon ja digiriigi kogukonna arendamine					
Privaatsuskaitse tehnoloogiate ja privaatsustehnika integreerimine E-ITS standardisse	Standardiarendus	E-ITS asub teadlikult toimetama	E-ITSis on (1) andmekaitsemoodul	2023	RIA
Privaatsuskaitse tehnoloogiate taasisikustamise riskide näidiste koostamine	Uuring	Aruanne pseudonüümimise ja nõrga anonüümisse taasidentifitseerimisest	100% rakenduses olevatest avaandmete anonüümimise meetoditest ei ole haavatavad aruandes olevatele rünnetele	2024	MKM
Privaatsuskaitse tehnoloogiate turu-uuring	Turu-uuring	Aruanne võtmetehnoloogiate pakkujate kohta	(1) turu-uuring riigi hankijatele saadaval	2024	MKM
Tõlkida ISO/IEC 27550 eesti keelde	Standardi ja terminoloogia tõlge eesti keelde	EVS standard + terminoloogia	(1) standard ja selle terminoloogia tõlgitud	2023	EVS
Tõlkida ISO/IEC 29134 eesti keelde	Standardi ja terminoloogia tõlge eesti keelde	EVS standard + terminoloogia	(1) standard ja selle terminoloogia tõlgitud	2023	EVS

ID D-16-215
Avalik

Tõlkida ISO/IEC 27701 eesti keelde	Standardi ja terminoloogia tõlge eesti keelde	EVS standard + terminoloogia	(1) standard ja selle terminoloogia tõlgitud	2024	EVS
Privaatsusmõju analüüside, privaatsustehnika ja konkreetse valdkonna privaatsuskaitse tehnoloogiate, psuedonüümimise vs anonüümimise koolitused andmekaitsespetsialistidele, teenusejuhtidele ja eetikakomiteede liikmetele	Koolitusmaterjalid ja koolitus	Riigiasutuste ja KOVide andmekaitsespetsialistid teavad, milliseid probleeme saab tehnoloogiatega lahendada ja milliseid minimeerimisega	(10) koolitatud asutust	2024	MKM
Andmete avaldamise tehnoloogiad - koolitused analüütikutele	Koolitusmaterjalid ja koolitus	Levib teadmus, kuidas isikustatud andmeid töödelda anonüümsemaks ning avaldada	(5) asutust hakkavad pärast koolitust privaatsuskaitse tehnoloogiad rakendama.	2024	RIA
Koolitus andmeanalüütikutele töövahenditest, andmekaitsest igapäevatöös, pseudonüümimise ja anonüümimise vahest	Koolitusmaterjalid ja koolitus	Levib teadmus, kuidas isikustatud andmeid avaldada	(10) asutusest on koolitusel osalejaid	2023	MKM/RIA
Andmejälgija ja nõusolekuteenuse integratsiooni koolitused	Andmejälgija ja nõusolekuteenuse integratsioon avaliku ja erasektori teenustesse	Koolitusmaterjalid	(10) asutusest on koolitusel osalejaid	2023	MKM/RIA

Teadlikkuse tõstmine oma andmetest ning andmehügieenist	Tõsta inimeste teadlikkust enda andmetega seotud riskidest, võimalustest ja kohustustest	Avalikus ruumis viiakse kolme kuni viie aasta jooksul läbi teavitusprogramm andmekaitse edulugudest.	Teavitatud on kanaleid kaudu, mis jõuavad koos üle (100 000) e-riigi kasutajani.	2024	MKM

Bibliograafia

[1] *Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[2] Johanna Vallistu, Tea Danilov ja Uku Varblane. *Andmeühiskonna tulevik. Stsenaariumid aastani 2035*. Tehniline raport. Arenguseire Keskus, 2022. URL: https://arenguseire.ee/wp-content/uploads/2022/12/2022_andmeyhiskonna-tulevik_raport.pdf.

[3] *Eesti digiühiskond 2030. Valdkonna arengukava*. Tehniline raport. Eesti Vabariigi Majandus- ja Kommunikatsiooniministeerium, 2021. URL: https://mkm.ee/digiriik-ja-uhenduvus/digiuhiskonna-arengukava-2030.

[4] The Royal Society. *From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis*. 2023. URL: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf?la=en-GB&hash=4769FEB5C984089FAB52FE7E22F379D6.

[5] Centre for Data Ethics ja Innovation's (CDEI). *Privacy Enhanching Technologies Adoption Guide*. 2021. URL: https://cdeiuk.github.io/pets-adoption-guide.

[6] United Nations Committee of Experts on Big Data ja New York Data Science for Official Statistics. *United Nations Guide on Privacy-Enhancing Technologies for Official Statistics*. United Nations, 2023. URL: https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf.

[7] Cybernetica AS. *Privaatsuskaitse tehnoloogiate kontseptsioon*. Tehniline raport. 2023.

[8] Kobbi Nissim *et al*. „Bridging the gap between computer science and legal approaches to privacy". *Harv. JL & Tech.* 31 (2017), lk. 687. URL: https://privacytools.seas.harvard.edu/files/privacytools/files/02.-article-wood-7.21.pdf.

[9] Rain Raa ja Kadri Siibak. „Pangasaladus". *Juridica* (2002), lk. 171–176. URL: https://www.juridica.ee/article.php?uri=2002_3_pangasaladus.

[10] Gerald Spindler ja Philipp Schmechel. „Personal Data and Encryption in the European General Data Protection Regulation". *JIPITEC* 7.2 (2016), lk. 163–177. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec7&div=18&id=&page=.

[11] X-eHealth, Vanja Pajić ja Klára Jiráková. *D4.2.1 - Information paper on the current challenges in legal aspects of cross-border exchange of personal data*. Information paper. 2021. URL: https://www.x-ehealth.eu/wp-content/uploads/2022/01/D4.2.1-%E2%80%93-Information-paper-on-the-current-challenges-in-legal-aspects-of-cross-border-exchange-of-personal-data.pdf.

[12] Monika Mikiver. *Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile*. Analüüs. 2021.

[13] Vabariigi Presidendi Kantselei avalike suhete osakond. *Piltuudis: President Ilves kohtus Euroopa Komisjoni digitaalarengu voliniku Neelie Kroesiga*. 2013. URL: https://vp2006-2016.president.ee/et/meediakajastus/pressiteated/9231-piltuudis-president-ilves-kohtus-euroopa-komisjoni-digitaalarengu-voliniku-neelie-kroesiga/index.html.

[14] Dan Bogdanov *et al*. „Students and Taxes: a Privacy-Preserving Study Using Secure Computation“. *Proc. Priv. Enhancing Technol.* 2016.3 (2016), lk. 117–135. DOI: 10.1515/popets-2016-0019.

[15] Mari Liis Räis, Epp Kallaste ja Siiri-Lii Sandre. *Haridusliku erivajadusega õpilaste kaasava hariduskorralduse uuring. Uuringu lõppraport*. Tehniline raport. Eesti Rakendusuuringute Keskus CentAR, 2016. URL: https://centar.ee/tehtud-tood/haridusliku-erivajadusega-opilaste-kaasava-hariduskorralduse-uuring.

[16] PRACTICE (FP7-ICT-2013-10). *D14.4 Validation Report*. Tehniline raport. 2016. URL: https://practice-project.technikon.com/downloads/publications/year3/D14.4-Validation-Report-PU-M36.pdf.

[17] PRACTICE (FP7-ICT-2013-10). *Pilot of the secure survey system created in PRACTICE*. 2016. URL: https://practice-project.technikon.com/blog/entry/pilot-of-the-secure-survey-system-created-in-practice.html.

[18] *IVXV raamistiku nõuded krüptosüsteemile*. URL: https://www.valimised.ee/sites/default/files/2021-10/IVXV%20raamistiku%20n%C3%B5uded%20kr%C3%BCptos%C3%BCsteemile.pdf.

[19] *IVXV arhitektuur Versioon 1.8.0*. Arhitektuuridokument. 2022. URL: https://www.valimised.ee/sites/default/files/2023-02/IVXV-arhitektuur.pdf.

[20] Dorel Hiir. „Innovatsioonivõimekuste arendamine läbi disainieksperimentide Politsei- ja Piirivalveameti näitel“. *Magistritöö* (2021). URL: https://digikogu.taltech.ee/et/Item/5838481f-f13e-4f43-8d56-363ed35299ee.

[21] European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Tehniline raport. 2020. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.